



Universidad
de Alcalá

LAS NUEVAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA LIMITATIVAS DEL DERECHO AL SECRETO DE LAS COMUNICACIONES EN EL PROCESO PENAL

**(THE NEW TECHNOLOGICAL INVESTIGATION MEASURES
LIMITING THE RIGHT TO PRIVACY OF COMMUNICATIONS IN
THE CRIMINAL PROCESS)**

Máster Universitario en Acceso a la Profesión de Abogado

Presentado por:

D^a SANDRA PÉREZ CHAMARRO

Dirigido por:

Dr. D. JOSÉ ANTONIO DEL OLMO DEL OLMO

Alcalá de Henares, a 1 de febrero de 2019

RESUMEN

A través del presente trabajo queremos realizar un análisis detallado de la reforma introducida por la Ley Orgánica 13/2015, de 5 de octubre, de la Ley de Enjuiciamiento Criminal, respecto a la regulación de las medidas de investigación tecnológica en el proceso penal, persiguiendo el fin de fortalecer las garantías procesales. El avance de las nuevas tecnologías en los últimos años ha tenido una gran repercusión en la sociedad y en el Derecho. En consecuencia, ha surgido la necesidad de adaptar nuestra legislación procesal penal a las nuevas formas de cibercrimen, lo cual se ha llevado a cabo mediante la reestructuración del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal.

ABSTRACT

By means of the present paper we want to make a detailed analysis of the reform introduced by the Organic Law 13/2015, October 5th, of the Criminal Procedure Act, regarding the regulation of technological investigation measures in the criminal process, pursuing the purpose of strengthening procedural guarantees. The advance of new technologies in recent years has had a great impact on society and Law. Consequently, the need to adapt our criminal procedure legislation to new forms of cybercrime has arisen, which has been carried out through the restructuring of Title VIII of Book II of the Criminal Procedure Act.

PALABRAS CLAVE

Medidas de investigación tecnológica. Proceso penal. Intervención de las comunicaciones. Derecho al secreto de las comunicaciones. Delitos informáticos. Ley de Enjuiciamiento Criminal. Reforma.

KEY WORDS

Technological research measures. Criminal process. Communication intervention. Right to privacy of communications. Cybercrime. Criminal Procedure Act. Reform.

ABREVIATURAS

LO	Ley Orgánica
TC	Tribunal Constitucional
TS	Tribunal Supremo
LECrim	Ley de Enjuiciamiento Criminal
CE	Constitución Española
DUE	Derecho de la Unión Europea.
DUDH	Declaración Universal de los Derechos Humanos
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
CEDH	Convenio Europeo de Derechos Humanos
TEDH	Tribunal Europeo de Derechos Humanos
CP	Código Penal
IP	Internet Protocol
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Station Equipment Identity
LGT	Ley General de Telecomunicaciones
UE	Unión Europea.
VIS	Sistema de Información de Visados.

ÍNDICE

RESUMEN.....	1
ABSTRACT.....	1
PALABRAS CLAVE	1
KEY WORDS	1
ABREVIATURAS	2
1.INTRODUCCIÓN.....	6
2.EVOLUCIÓN HISTÓRICA.	7
3.PRESUPUESTOS COMUNES PARA LA ADOPCIÓN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA.....	9
3.1.Procedimiento de adopción.....	11
3.2.Duración.....	12
3.3.Control y uso de la información.....	13
4.LA INTERVENCIÓN JUDICIAL DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS. ANTECEDENTES HISTÓRICOS, GÉNESIS Y EVOLUCIÓN EN LA REGULACIÓN ACTUAL.	16
4.1.Antecedentes históricos y evolución actual.....	16
4.2.Intervenciones telefónicas: disposiciones generales.	17
4.2.1.Presupuestos de la medida y delimitación objetiva y subjetiva.	19
4.2.2.Solicitud de autorización judicial de la medida.	23
4.2.3.El deber de colaboración.	26
4.2.5.Control de la intervención y el acceso de las partes a las grabaciones.	27
4.2.6.Valor probatorio de la medida.....	30
4.3.Incorporación al proceso de datos electrónicos de tráfico o asociados.....	32

4.4. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.....	33
4.4.1. Identificación mediante número IP... ..	33
4.4.2. Identificación de los terminales mediante los códigos IMSI e IMEI.....	33
4.4.3. Identificación de titulares o terminales o dispositivos de conectividad.	35
4.5. La interceptación de las comunicaciones de WhatsApp.....	36
4.6. Supuestos controvertidos de intervención de las comunicaciones.....	38
5. RÉGIMEN JURÍDICO DE LA CAPTACIÓN Y GRABACIÓN DE COMUNICACIONES ORALES MEDIANTE LA UTILIZACIÓN DE DISPOSITIVOS ELECTRÓNICOS.....	42
5.1. Grabación de las comunicaciones orales directas.....	43
5.2. Presupuestos.....	44
5.3. Contenido de la resolución judicial.....	45
5.4. Control de la medida.....	45
5.5. Cese.....	46
5.6. Casos susceptibles de grabación de las comunicaciones orales.....	46
5.6.1. Utilización de micrófonos.	46
5.6.2. Utilización de cámaras ocultas.....	48
6. RÉGIMEN JURÍDICO DE LA UTILIZACIÓN DE DISPOSITIVOS TÉCNICOS DE CAPTACIÓN DE LA IMAGEN, DE SEGUIMIENTO Y DE LOCALIZACIÓN.....	50
6.1. Captación de imágenes en lugares o espacios públicos.....	50
6.2. Utilización de dispositivos o medios técnicos de seguimiento y localización.....	50
7. RÉGIMEN JURÍDICO DEL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN.....	52
7.1. Ámbito de la medida.....	54

7.2.Necesidad de motivación individualizada.....	54
7.3.Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.....	56
7.4.Autorización judicial.....	57
8.RÉGIMEN JURÍDICO DE LOS REGISTROS REMOTOS SOBRE EQUIPOS INFORMÁTICOS.....	59
8.1.Presupuestos.....	59
8.2.Deber de colaboración.....	61
8.3.Duración de la medida.....	61
8.4.Técnicas de obtención de información a través de registros remotos sobre dispositivos informáticos.....	62
9.CONCLUSIONES.....	64
BIBLIOGRAFÍA	67

1. INTRODUCCIÓN.

El avance de las nuevas tecnologías producido durante los últimos años ha puesto de manifiesto la insuficiencia de la normativa ya existente, concebida para otros tiempos. En consecuencia, surge así la necesidad de una reforma de la Ley de Enjuiciamiento Criminal (LECrim), operada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Previamente, tanto la doctrina como la jurisprudencia ya habían proclamado la necesidad de reformar trascendentalmente el cuadro normativo existente para adaptarlo a la realidad de nuestros tiempos.

Han sido distintos los aspectos jurídicos objeto de reforma, entre los que destacan las medidas de investigación tecnológica en el proceso penal. La citada LO 13/2015, a partir del apartado 7 de su artículo único, introduce una nueva redacción del Título VIII del Libro II de la LECrim, creando diez capítulos. Tales cuestiones novedosas serán objeto de este estudio, más concretamente los capítulos IV a X, relativos a las siguientes diligencias de investigación: la interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; el registro de dispositivos de almacenamiento masivo de información; y los registros remotos sobre equipos informáticos. Además, se analizarán las disposiciones comunes a todas dichas medidas de investigación tecnológica, así como las medidas para su aseguramiento.

Todas las citadas cuestiones se estudiarán rigurosamente, atendiendo a sus antecedentes históricos y evolución actual, todo ello poniendo exhaustivo énfasis en la doctrina y a la jurisprudencia existente. Finalmente, se dedicará un apartado a la problemática derivada de las medidas de investigación tecnológica y se expondrán las conclusiones a las que se ha llegado tras el estudio de la materia expuesta en este trabajo.

2. EVOLUCIÓN HISTÓRICA.

Hasta la reforma operada por la LO 13/2015, la LECrim tan sólo regulaba la entrada y registro en lugar cerrado, de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica (antiguo Título VIII del Libro II de la LECrim).

Así las cosas, la interceptación de las comunicaciones telefónicas y telemáticas no se encontraba regulada en la norma procesal, lo que suponía la existencia de impedimentos para llevar a cabo este tipo de investigaciones que incidían gravemente en el derecho al secreto de las comunicaciones del art. 18.3 de la Constitución Española (CE). Tales deficiencias tuvieron que ser suplidas por un consolidado cuerpo jurisprudencial del Tribunal Constitucional (TC) y del Tribunal Supremo (TS), atendiendo a las necesidades de persecución de la delincuencia tecnológica y dando cobertura legal a unos supuestos que el legislador no había previsto específicamente en su tiempo.

La imperiosa necesidad de llevar a cabo una reforma de la LECrim fue evidenciada en la Sentencia 145/2014 de la Sala 2ª del TC de 22 de septiembre de 2014. En dicha sentencia, el TC estimó parcialmente un recurso de amparo interpuesto por falta de garantías constitucionales, indicando que las escuchas realizadas a los detenidos en los calabozos donde se encontraban carecían de habilitación legal, aunque contasen con autorización judicial que autorizaba a la instalación de "arteficios técnicos de escucha, grabación de sonido e imagen". El TC quiso reflexionar sobre la importancia de reserva de Ley como garantía de seguridad jurídica en el ámbito de los derechos fundamentales y libertades públicas, así como concluir que la suplencia de los defectos de la Ley *"no puede ser trasladada a un escenario de injerencia en el secreto de las comunicaciones en el que no exista previsión legal alguna, o en el que, cuando menos, tal regulación no se corresponde con la que se identifica y cita en las resoluciones recurridas.....al no ser el art. 579.2 LECrim. la disposición jurídica a considerar, no puede otorgar tampoco esa norma garantía alguna frente a posibles abusos, ni aportar al individuo una protección adecuada contra la arbitrariedad"*¹.

La respuesta a esta exigencia se ha producido a través de la LO 13/2015, refiriéndose su preámbulo a la sentencia del TC anteriormente citada: *el Tribunal Constitucional ha*

¹ MARTÍN MARTÍN DE LA ESCALERA, A.M., *El registro de dispositivos de almacenamiento masivo de la información*. Pág. 3 y 4.

apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal.

A través de la iniciativa legislativa citada se aborda la regulación de las medidas de investigación tecnológica. Actualmente, el nuevo Título VIII se divide en diez capítulos, reestructurando el contenido del antiguo título en tres capítulos nuevos, y añadiendo algunas novedades referentes a las medidas de investigación tecnológica. La nueva estructura ha quedado del siguiente modo:

- Capítulo I: De la entrada y registro en lugar cerrado.
- Capítulo II: Del registro de libros y papeles.
- Capítulo III: De la detención y apertura de la correspondencia escrita y telegráfica
- Capítulo IV: Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.
- Capítulo V: La interceptación de las comunicaciones telefónicas y telemáticas.
- Capítulo VI: Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.
- Capítulo VII: Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.
- Capítulo VIII: Registro de dispositivos de almacenamiento masivo de información.
- Capítulo IX: Registros remotos sobre equipos informáticos.
- Capítulo X: Medidas de aseguramiento.

3. PRESUPUESTOS COMUNES PARA LA ADOPCIÓN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA.

La LECrim regula en el Capítulo IV del Título VIII del Libro II las disposiciones comunes aplicables a las medidas de investigación tecnológica (arts. 588 bis. a y ss. LECrim). Tales preceptos fueron introducidos por el apartado trece del artículo único de la LO 13/2015.

Dichas medidas de investigación tecnológica son las siguientes:

- La interceptación de las comunicaciones telefónicas y telemáticas.
- La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.
- La utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen.
- El registro de dispositivos de almacenamiento masivo de información.
- Los registros remotos sobre equipos informáticos.

Cualquiera de las citadas medidas puede ser adoptada durante la fase de instrucción del proceso penal, mediante autorización judicial. Tal autorización debe atender a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida (art. 588 bis a. 1).

- **Especialidad:** la medida debe estar en relación con la investigación del delito, quedando prohibida toda medida cuyo fin sea prevenir o descubrir delitos o despejar sospechas sin base objetiva (art. 588 bis a. 2).

En este sentido, la medida debe ser delimitada objetivamente (precisión del hecho investigado) y subjetivamente (identificación del sospechoso), vinculando con el sujeto las líneas telefónicas que se pretende intervenir. A tal fin, el juez tendrá que contar con indicios suficientes de la comisión del delito y de la participación del investigado².

² FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A. *Cuestiones actuales del Derecho Procesal*. Edit. Dykinson, Barcelona, 2015. Pág. 130.

- **Idoneidad:** este principio limita el ámbito objetivo y subjetivo de la medida, así como su duración conforme a su utilidad (art. 588 bis a. 3).
- **Excepcionalidad y necesidad:** la LECrim establece unos presupuestos en los que sólo podrán adoptarse las medidas de investigación tecnológica (art. 588 bis a. 4):
 - a) Cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o
 - b) Cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

Respecto a la idoneidad, excepcionalidad y necesidad, la medida sólo podrá acordarse cuando no existan otras menos gravosas para los derechos fundamentales del investigado e igualmente útiles para la investigación. Para ello, deben constar en la resolución judicial los hechos en los que el juez apoya la valoración de estos tres aspectos. Además, si resultare necesario, podrá contener una valoración específica de la situación. Si el juez no realizara tal motivación, no sería válida una autorización mecánica ante la solicitud policial, sin haberse producido una valoración de los principios citados³.

- **Proporcionalidad:** este principio se cumplirá si la adopción de las medidas de investigación, en atención a todas las circunstancias del caso, resultan útiles para el interés público y de terceros, sin que sea superior el sacrificio de los derechos e intereses afectados por las mismas. Será preciso realizar una ponderación de los intereses en conflicto, para lo cual se valorará el interés público con respecto a la gravedad del hecho, su trascendencia social o el ámbito

³ Ídem.

tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

3.1.Procedimiento de adopción.

Las medidas de investigación deben ser adoptadas por el juez, de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial (art. 588 bis b, apartado 1 LECrim). En este último caso, la solicitud deberá contener los siguientes aspectos (art. 588 bis b, apartado 2 LECrim):

- 1) La descripción del hecho y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
- 2) La motivación de la necesidad de la medida y de los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.
- 3) Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.
- 4) La extensión de la medida con especificación de su contenido.
- 5) La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.
- 6) La forma de ejecución de la medida.
- 7) La duración de la medida que se solicita.
- 8) El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Presentada la solicitud y oído el Ministerio Fiscal, el juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado, en el plazo máximo de veinticuatro horas desde la presentación de la solicitud. Dicho plazo podrá ser interrumpido si el juez considerase necesaria una ampliación o aclaración de los términos de la solicitud a fin de comprobar el cumplimiento de alguno de los requisitos exigidos para la misma (art. 588 bis c, apartados 1 y 2 LECrim).

El auto del juez que autorice la medida debe contener los siguientes extremos (art. 588 bis c, apartados 3 LECrim):

- a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.
- b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.
- c) La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.
- d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.
- e) La duración de la medida.
- f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.
- g) La finalidad perseguida con la medida.
- h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Podrán acordarse las medidas de investigación cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas (art. 588 bis h LECrim).

Ha de indicarse que tanto la solicitud de la medida, como las actuaciones posteriores, serán sustanciadas en pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa (art. 588 bis d LECrim).

3.2.Duración.

La autorización judicial de la medida indicará la duración de la misma, no pudiendo exceder del tiempo imprescindible para el esclarecimiento de los hechos (art. 588 bis e, apartado 1 LECrim).

No obstante, el juez, mediante auto motivado, podrá **prorrogar** la duración de la medida, ya sea de oficio o a petición razonada del solicitante, siempre que subsistan las causas que la motivaron (art. 588 bis e, apartado 2 LECrim).

Para el caso de que el Ministerio Fiscal o la Policía Judicial soliciten la prórroga de la duración de la medida, deberán dirigirse al juez con la antelación suficiente a la expiración del plazo concedido. La solicitud deberá incluir:

- a) Un informe detallado del resultado de la medida.
- b) Las razones que justifiquen la continuación de la misma.

El juez, mediante auto motivado, debe resolver en el plazo de dos días siguientes a la presentación de la solicitud, pudiendo solicitar aclaraciones o mayor información. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada (art. 588 bis f LECrim).

Una vez transcurrido el plazo de duración inicial concedido o finalizado el tiempo de prórroga, la medida cesará a todos los efectos (art. 588 bis e, apartado 3 LECrim).

Otra forma de cese de la medida se produce cuando desaparecen las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos, y así es acordado por el juez (art. 588 bis j LECrim).

3.3.Control y uso de la información.

La Policía Judicial será la encargada del control de la medida, debiendo informar al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma (art. 588 bis g LECrim).

Conforme a la jurisprudencia del TS, la doctrina viene entendiendo como “**cadena de custodia** el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba. Esta Sala tiene establecido que la integridad de la cadena de custodia garantiza que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del Tribunal no sufre alteración alguna. Al tener que circular o transitar por diferentes lugares los efectos o enseres intervenidos en el curso de la investigación, es necesario para que se emitan los dictámenes

periciales correspondientes tener la seguridad de que lo que se traslada es lo mismo en todo momento, desde que se interviene hasta el momento final que se estudia y analiza y, en su caso, se destruye”⁴.

El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularán conforme al art. 579 bis (art. 588 bis i LECrim). En este punto cabe señalar los problemas que plantea la iniciación de un proceso penal a partir de las informaciones obtenidas en otra causa, basados en indicios de delito obtenidos a través de una intervención telefónica previa. La jurisprudencia del TS no tiene un único criterio consolidado al respecto, entendiendo en algunas ocasiones que la nueva causa tiene una dependencia absoluta respecto de las intervenciones practicadas en la anterior, debiendo el juez controlar la validez jurídica de aquéllas a la hora de valorar las pruebas practicadas en el segundo proceso⁵, y en otras defiende la autonomía entre ambos procedimientos⁶.

Por último, respecto a la **destrucción de los registros**, los originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida serán destruidos una vez que se ponga término al procedimiento mediante resolución firme. Dicha eliminación será ordenada por el tribunal a la Policía Judicial. No obstante, se conservará una copia bajo custodia del Letrado de la Administración de Justicia, la cual será destruida cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal (art. 588 bis k LECrim).

Es importante recordar que *“la regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza o elemento de convicción intervenido; se asegura de esa forma que lo que se analiza es justamente lo ocupado y que no ha sufrido alteración alguna (STS 1072/2012, de 11-12)”⁷*. En consecuencia, la ruptura en la cadena de custodia repercutirá directamente sobre la fiabilidad y autenticidad de las pruebas. Además, dicha ruptura podrá

⁴ STS 747/2015, de 15 de noviembre, FJ 6.

⁵ STS 1769/2003, de 29 de diciembre, FJ 2.

⁶ STS 688/2008, de 30 de octubre, FJ 1.

⁷ STS 747/2015, de 15 de noviembre, FJ 6.

vulnerar el derecho a la presunción de inocencia: *“Y también se ha advertido que la ruptura de la cadena de custodia puede tener una indudable influencia en la vulneración del derecho a la presunción de inocencia, pues resulta imprescindible descartar la posibilidad de que la falta de control administrativo o jurisdiccional sobre las piezas de convicción del delito pueda generar un equívoco o un error sobre cualquier dato decisivo para el juicio de tipicidad. Lo contrario podría implicar una más que visible quiebra de los principios que definen el derecho a un proceso justo”*⁸.

⁸ Ídem.

4. LA INTERVENCIÓN JUDICIAL DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS. ANTECEDENTES HISTÓRICOS, GÉNESIS Y EVOLUCIÓN EN LA REGULACIÓN ACTUAL.

La interceptación de las comunicaciones telefónicas y telemáticas se encuentra regulado en el Capítulo V del Título VIII del Libro II de la LECrim, introducido por el apartado catorce del artículo único de la Ley Orgánica 13/2015.

4.1. Antecedentes históricos y evolución actual.

La regulación anterior a la reforma de la LECrim operada por la LO 13/2015 resultaba escasa, ya que no contenía ninguna referencia a las medidas de investigación tecnológica, lo que provocaba que se produjeran, frecuentemente, vulneraciones del derecho al secreto de las comunicaciones (art. 18.3 CE) con la práctica de la medida de interceptación de las comunicaciones telefónicas y telemáticas.

Mediante la nueva regulación recogida en nuestro texto procesal penal se pretende ofrecer una regulación más rigurosa y garantista de las intervenciones telefónicas y telemáticas en el proceso penal. Esta necesidad ya había sido exigida por el TS, TC y TEDH en numerosas sentencias de los últimos años⁹.

La importancia de la reforma trasciende a la adaptación de la norma procesal a la realidad tecnológica actual, ya que con los recientes avances tecnológicos no tendría sentido hablar sólo de intervenciones telefónicas, puesto que en nuestras comunicaciones diarios utilizamos diversos nuevos sistemas de comunicación telemática.

La introducción de los arts. 588 ter a) a 588 ter m) tiene causa en el afán de proporcionar una mejor protección del derecho al secreto de las comunicaciones y del tratamiento de los datos asociados con la práctica de las intervenciones. Hasta entonces, los jueces de instrucción han autorizado la intervención de las comunicaciones de forma genérica, haciendo referencia únicamente a las comunicaciones telefónicas y omitiendo lo referente a la cesión del resto de datos electrónicos del intervenido.

⁹ SSTs 413/2015, de 30 de junio; 128/2015, de 5 de febrero; 250/2014, de 14 de marzo; y 712/2012, de 26 de septiembre. SSTC 184/2003, de 23 de octubre; 26/2006, de 30 de enero; y 145/2014, de 22 de septiembre; y STEDH de 18 de febrero de 2003 (asunto Prado Bugallo contra España).

4.2. Intervenciones telefónicas: disposiciones generales.

La Sección I del Capítulo V del Título VIII del Libro II de la LECrim recoge las disposiciones generales aplicables a la interceptación de las comunicaciones telefónicas y telemáticas, las cuales serán analizadas a continuación.

El secreto de las comunicaciones telefónicas es un derecho fundamental garantizado por la CE en el art. 18.3. Además, el art. 12 de la Declaración Universal de los Derechos Humanos (DUDH) y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), hacen referencia al derecho a no ser objeto de injerencias arbitrarias o ilegales en la vida privada y en la correspondencia. A su vez, el art. 8.1 del Convenio Europeo de Derechos Humanos (CEDH) dispone que *“toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”*. Añade el art. 8.2 del CEDH *“que no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho (respeto a la vida privada y familiar, domicilio y correspondencia) sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”*.

Sin embargo, el secreto a las comunicaciones telefónicas no es un derecho absoluto, sino que puede verse limitado y restringido, debiendo tales limitaciones y restricciones estar previstas en la ley. Dichas medidas deben ser proporcionadas en cada caso concreto, perseguir un fin legítimo y resultar necesarias respecto a las circunstancias de la investigación y del hecho investigado. En consecuencia, se valorará la gravedad del delito, los indicios de su existencia y la intervención del sospechoso, y la necesidad de la medida¹⁰.

La previsión legal en nuestro Derecho que habilita a la aplicación de la medida limitativa del derecho del art. 18.3 CE se encuentra contenida en el art. 588 ter a LECrim. No obstante, España ha sido condenada en numerosas ocasiones por el Tribunal Europeo de Derechos Humanos (TEDH) por vulneración del derecho al secreto de las comunicaciones telefónicas, al considerar éste insuficiente la regulación al respecto y que no cumple las exigencias

¹⁰ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 129.

establecidas en la jurisprudencia de dicho Tribunal¹¹. En contraposición, el TC¹² defiende que, si en la práctica de la medida en el caso concreto se cumple con las condiciones materiales exigidas por la ley, no puede hablarse de la existencia de una vulneración real del derecho del afectado al secreto de sus comunicaciones telefónicas, ya que su esfera esencial habría permanecido intacta. Por ello, no hay que olvidar la importancia que tiene la resolución judicial para dar validez a una intervención telefónica cuya regulación legal había sido insuficiente hasta la reforma operada por la Ley Orgánica 13/2015¹³.

En la STS 747/2017, de 21 noviembre, se resuelve desestimando un recurso de casación interpuesto por los acusados en un procedimiento de delitos contra la salud pública. Es habitual que en este tipo de delitos se lleven a cabo intervenciones telefónicas para su investigación. En el recurso interpuesto por los condenados en segunda instancia, éstos criticaron las intervenciones telefónicas, reclamando su nulidad y, como consecuencia, la inutilizabilidad de las pruebas derivadas, lo que llevaría a un desierto probatorio.

La intervención telefónica acordada tuvo lugar en otra causa anterior, lo que llevaría a que la autorización judicial inicial careciera de uno de los requisitos esenciales e inmanente a toda injerencia en el derecho al secreto de las comunicaciones: la proporcionalidad. Para que la suspensión de un Derecho Fundamental de tal importancia sea ajustada a derecho debe existir una razón poderosa, la cual podría ser la investigación de un delito, pero solo cuando la infracción penal reviste cierta "gravedad". La causa donde se acordó la medida de investigación trataba de un delito de robo con violencia. Conforme a la catalogación del CP (arts. 13 y 33), es un delito menos grave, por lo que no podría servir de fundamento a una medida tan invasiva en un derecho fundamental como lo es la intervención de las comunicaciones telefónicas. En estos casos, se exige un juicio de proporcionalidad: *“solo la averiguación y sanción de delitos de cierta entidad -nunca un delito de bagatela - puede justificar ese tipo de injerencia en una sociedad democrática... Solo cuando la gravedad de la infracción lo aconseje y justifique es legítima una intervención telefónica. Un delito de escasa entidad no habilita para la adopción de esa medida. La necesaria tarea de ponderación ha de decantarse en esos casos por la*

¹¹ STEDH, de 18 de febrero de 2003, asunto Prado Bugallo contra España; STEDH, de 16 de febrero de 2000, asunto Amann contra Suiza.

¹² STC 39/1999, de 22 de marzo.

¹³ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 129.

prevalencia de la efectividad de los derechos fundamentales, frente al interés en la persecución de los delitos” (FJ 2). Esta exigencia la podemos encontrar en la jurisprudencia del TEDH¹⁴.

No obstante lo anterior, es necesario matizar el concepto de “gravedad”. No debemos analizar únicamente la magnitud de la sanción o si se trata de una categoría específica de infracciones según la taxonomía del Código Penal; sino que han de manejarse otros criterios: afectación social, repercusión en la convivencia, significado y rango en un estado de derecho de los bienes jurídicos lesionados, morfología de la infracción. En palabras del TS, *“Una intervención telefónica podría no estar justificada para investigar un delito que tutela bienes primordialmente individuales (un hurto, v.gr); y, en cambio, sí estarlo para delitos con pena “menos grave” (algunos cohechos, delitos cometidos por funcionarios públicos...) ora por el interés colectivo en el bien afectado; ora por la actuación coordinada de los plurales sujetos activos (entramado organizativo). Trascendencia, repercusión social y modalidad delictiva más o menos compleja son elementos a sopesar, y no solo el tamaño de la pena”*.

En el recurso de casación planteado, el Tribunal concluyó que *“No podemos negar aquí la presencia de ese presupuesto en la intervención telefónica decretada en otro procedimiento judicial seguido por un delito de robo con violencia. Es un delito menos grave, sí, según la etiquetación legal. Pero a estos efectos no es a esa gravedad la que hay que atender, como viene subrayando la jurisprudencia constitucional y como confirma ahora la lectura del art. 588 bis a) 5 LECrim, que se refiere a la gravedad del hecho y no a la naturaleza grave del delito”*. Por tanto, a la hora de ponderar la proporcionalidad de la medida, y en especial la existencia del presupuesto de gravedad, debemos atender a la gravedad del hecho, y no a la del delito.

4.2.1. Presupuestos de la medida y delimitación objetiva y subjetiva.

La autorización judicial que habilita a la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación (art. 588 ter a LECrim).

¹⁴ SSTEDH de 19 de abril de 2001, Peers v. Grecia; 24 de julio de 2001, Velainas v. Lituania; 11 de diciembre de 2003, Basan v. Italia; o 24 de febrero de 2005, Jaskaukas v. Lituania.

El art. 579.1 LECrim enumera los siguientes delitos como objeto de una investigación en la que se requiera efectuar una intervención telefónica:

- 1) Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
- 2) Delitos cometidos en el seno de un grupo u organización criminal.
- 3) Delitos de terrorismo.

Podemos observar que el ámbito objetivo de aplicación de la medida es bastante extenso, debiendo prestar especial atención cuando se trate delitos cometidos informáticamente, no autorizándose la intervención de las comunicaciones cuando el delito no tenga mucha trascendencia.

A la hora de acordar la medida, deben existir, al menos, indicios suficientes fundados de la participación de una persona en la comisión de un delito. De conformidad con la STS 747/2017, de 21 de noviembre, en su FJ 4: *“Para que sea constitucionalmente legítima una injerencia en el derecho al secreto de las comunicaciones, el Juez ha de verificar la presencia de unos indicios constatables por un tercero que rebasen el dintel de las meras sospechas y gocen de cierta potencialidad acreditativa; y que, sin llegar a constituir prueba, representen mucho más que una conjetura. No bastan afirmaciones apodícticas de sospecha. El órgano judicial ha de valorar no sólo la gravedad y naturaleza de los delitos que se pretende indagar; y la necesidad de la invasión de un derecho fundamental para esa investigación. Es imprescindible que efectúe un juicio ponderativo sobre el nivel cualificativo de los indicios que avalan las sospechas. La suficiencia de los indicios para llegar a afirmar la probabilidad de esas conclusiones justificativas de las escuchas no puede descansar exclusivamente en los agentes policiales. La constatación de la solidez de esos indicios es parte esencial del proceso discursivo y valorativo que debe realizar el Juez antes de conceder la autorización”*.

Sobre esta cuestión, la STC 197/2009, de 28 de septiembre, contiene una buena síntesis de esa reiterada y conocida doctrina:

“Desde la STC 49/1999, de 5 de abril (RTC 1999, 49), FJ 7, este Tribunal viene afirmando que forman parte del contenido esencial del art. 18.3 CE (RCL 1978, 2836) las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga. Éstas deben explicitar, en el momento de la adopción de la medida, todos los

elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida pues, por la propia finalidad de ésta, la defensa no puede tener lugar en el momento de su adopción (SSTC 299/2000, de 11 de diciembre (RTC 2000, 299) , FJ 4 ; 167/2002, de 18 de septiembre (RTC 2002, 167) , FJ 2).

En primer lugar, la resolución judicial que acuerda una intervención telefónica ha de justificar la existencia de los presupuestos materiales habilitantes de la intervención: los datos objetivos que puedan considerarse indicios de la posible comisión de un hecho delictivo grave y de la conexión de las personas afectadas por la intervención con los hechos investigados. Indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento. La relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control, y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona. Esta mínima exigencia resulta indispensable desde la perspectiva del derecho fundamental, pues si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones, tal y como la CE (RCL 1978, 2836) lo configura, quedaría materialmente vacío de contenido...

Se trata, por consiguiente, de determinar si en el momento de pedir y adoptar la medida de intervención se pusieron de manifiesto ante el Juez, y se tomaron en consideración por éste datos objetivos que permitieran precisar que dicha línea era utilizada por las personas sospechosas de la comisión del delito o de quienes con ella se relacionaban, y que, por lo tanto, no se trataba de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan en los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional.

Sobre esa base, el Tribunal ha considerado insuficiente la mera afirmación de la existencia de una investigación previa, sin especificar en qué consiste, ni cuál ha sido su

resultado por muy provisional que éste pueda ser, afirmando también que la concreción del delito que se investiga, las personas a investigar, los teléfonos a intervenir y el plazo de intervención no pueden suplir la carencia fundamental de la expresión de los elementos objetivos indiciarios que pudieran servir de soporte a la investigación, ni la falta de esos indispensables datos pueda ser justificada a posteriori por el éxito de la investigación misma...También ha destacado el Tribunal que "la idea de dato objetivo indiciario tiene que ver con la fuente de conocimiento del presunto delito, cuya existencia puede ser conocida a través de ella. De ahí que el hecho en que el presunto delito puede consistir no pueda servir como fuente de conocimiento de su existencia. La fuente del conocimiento y el hecho conocido no pueden ser la misma cosa".

Por otro lado, cabe añadir que la medida contenida en el art. 588 ter LECrim afecta no sólo a las intervenciones telefónicas, sino también a las telemáticas, tales como a la mensajería privada enviada por chat, correo electrónico, SMS, fax, etc¹⁵.

Actualmente, los medios tecnológicos tienen una notoria presencia en nuestra vida personal y laboral, llegando a resultar su uso imprescindible. En cuanto al ámbito de las comunicaciones, han ido apareciendo nuevos sistemas tales como las aplicaciones de mensajería instantánea, entre las que cabe destacar WhatsApp. Más adelante profundizaremos en el estudio de la intervención de las comunicaciones efectuadas a través de dicha aplicación como medida de investigación tecnológica.

Respecto al **ámbito subjetivo**, existe una relación entre el sujeto y el dispositivo de la comunicación. La intervención se hará respecto de los terminales o medios de comunicación habitual u ocasionalmente utilizados por el investigado. La autorización podrá dar acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación¹⁶, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el

¹⁵ JAÉN VALLEJO, M. y PERRINO PÉREZ, A.L., "Medidas de investigación tecnológica" en *La Reforma Procesal Penal de 2015*. Dykinson, Madrid, 2015. Pág. 152.

¹⁶ En este artículo, se entiende por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

investigado sea titular o usuario. Por tanto, lo que importa no es tanto la titularidad sino la utilización del dispositivo de comunicación. Además, también es posible intervenir los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad (art. 588 ter b LECrim).

Por otro lado, la norma procesal también recoge la posibilidad de acordar la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona. Para ello debe concurrir alguno de los siguientes supuestos:

- 1) Que exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o
- 2) Que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular (art. 588 ter c LECrim).

4.2.2. Solicitud de autorización judicial de la medida.

El art. 588 ter d LECrim establece que la solicitud de autorización judicial deberá contener, además de los requisitos comunes de aplicación a todas las medidas (art. 588 bis b LECrim), los siguientes:

- a) La identificación del número de abonado, del terminal o de la etiqueta técnica,
- b) La identificación de la conexión objeto de la intervención o
- c) Los datos necesarios para identificar el medio de telecomunicación de que se trate.

En cuanto a la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:

- a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.
- b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

- c) La localización geográfica del origen o destino de la comunicación.
- d) El conocimiento de otros datos de tráfico asociados o no asociados, pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.

Puede ocurrir que, en el curso de unas intervenciones telefónicas legítimas aparezcan indicios de la comisión de otro delito, hecho del cual habría que dar cuenta al instructor para que decida si la medida se extiende o no a ese nuevo objeto procesal. Para ello, habrá que evaluar la gravedad de la nueva infracción. Mientras el Instructor toma una decisión, entiende el TS es su Sentencia 747/2017, de 21 de noviembre, FJ 6, que las escuchas no deben quedar en suspenso o que, de aparecer nuevos datos, sean inutilizables: *“La decisión final del instructor habrá de ser adoptada en un plazo prudencial y permitirá no solo la investigación de ese delito (hallazgo casual) sino además usar para acreditarlo los frutos de las escuchas; también de aquéllas producidas en ese periodo intermedio además de las iniciales en las que aparecieron esos indicios de una nueva infracción. No han de apartarse absurdamente las conversaciones intermedias. Contaban con autorización judicial. Mucho menos podemos derivar de ahí la ilegalidad de las posteriores conversaciones producidas cuando ya se había oficializado la investigación por la nueva infracción incoándose un nuevo procedimiento ad hoc. Esas conversaciones de las que surgieron indicios en la comisión de un delito contra la salud pública contaba con respaldo judicial como ya se ha dicho, por contra de lo que aducen algunos recurrentes”*.

Como norma general, la autorización de la medida se realizará por auto judicial motivado, salvo en caso de urgencia (cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la adopción de la medida), que podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

Respecto a la motivación del auto, la STS 395/2016, de 10 de mayo, FJ 1, indica que no es necesaria una justificación fáctica exhaustiva en el momento inicial en que se acuerda la medida en el procedimiento, ya que se encamina a profundizar en una investigación no acabada. En relación al contenido del auto, establece que TS que *“La motivación de los autos de intervención debe estar por encima de las meras hipótesis subjetivas o la simple plasmación de una suposición o incluso la convicción de la existencia de un delito y de la intervención en él del sospechoso, pues de aceptarse tal situación la invasión de la esfera de intimidad dependería exclusivamente de la voluntad del investigador, sin exigencias de justificación objetiva de ninguna clase, lo que no es admisible en un sistema de derecho y libertades efectivas, amparados en un razonable control sobre el ejercicio de los poderes públicos... Las resoluciones judiciales que autorizan la intervención o su prórroga forman parte del contenido esencial del art. 18.3 C.E ., y en dichas resoluciones se debe explicitar en el momento de adopción de la medida, los elementos indispensables para realizar el juicio de proporcionalidad, y su posible control posterior, ya que el afectado por la medida no puede alegar nada en el momento de su adopción. Los indicios objetivos se han de referir a la comisión de un delito y a la posible participación del sospechoso”*.

En la STS 404/2016 de 11 de mayo, FJ 4, el Tribunal recuerda que la jurisprudencia del TS y del TC considera que la motivación de la resolución judicial que acuerda las intervenciones constituye una exigencia inexcusable por la necesidad de justificar el presupuesto legal habilitante de la intervención (STC 253/2006, de 11 de septiembre). No obstante, en cuanto al contenido de la motivación, el TS indica que *“También constituye doctrina jurisprudencial consolidada que en el momento inicial del procedimiento, en el que ordinariamente se acuerda la intervención telefónica, no resulta exigible una justificación fáctica exhaustiva, pues se trata de una medida adoptada, precisamente, para profundizar en una investigación no acabada (Sentencias Sala Segunda Tribunal Supremo núm. 1240/98, de 27 de noviembre , núm. 1018/1999, de 30 de septiembre , núm. 1060/2003, de 21 de julio , núm. 248/2012, de 12 de abril , núm. 492/2012, de 14 de junio y núm. 301/2013, de 18 de abril , entre otras), por lo que únicamente pueden conocerse unos iniciales elementos indiciarios”*.

Es por ello que será suficiente que la motivación fáctica de las autorizaciones de este tipo de medida se fundamente en la remisión a los correspondientes antecedentes obrantes en las actuaciones y concretamente a los elementos fácticos que consten en la correspondiente solicitud policial, o en el informe o dictamen del Ministerio Fiscal, cuando se ha solicitado y

emitido. Hay que tener en cuenta que la motivación por remisión no es una técnica jurisdiccional modélica, en tanto que la autorización judicial debería ser auto suficiente. Pero el TS recuerda que *“La doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada sí, integrada con la solicitud policial, a la que se remite, o con el informe o dictamen del Ministerio Fiscal en el que solicita la intervención (STS núm. 248/2012, de 12 de abril), contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (doctrina jurisprudencial ya citada, por todas STC 72/2010, de 18 de octubre)”*. En consecuencia, la técnica de motivación por remisión será admisible siempre que la resolución judicial contenga todos los elementos necesarios para poder realizar el juicio de proporcionalidad.

4.2.3. El deber de colaboración.

El art. 588 ter e LECrim obliga a todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones. Además, dichos sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. En caso de incumplimiento de alguno de los deberes descritos, los sujetos obligados incurrirían en delito de desobediencia.

La colaboración con la justicia, por tanto, se extiende a las compañías de telefonía, almacenamiento, acceso a internet, y administradores de sitios web como redes sociales o foros, debiendo todos estos ceder datos personales y/o de conexión en todos los casos en que les sean requeridos¹⁷.

En cuanto a las autoridades respecto a las que hay que prestar colaboración, suscita especial interés el Ministerio Fiscal. La intervención de las telecomunicaciones es autorizada por el juez, siendo normalmente la Policía Judicial quien, en delegación de aquél, ejecuta la

¹⁷ RUBIO ALAMILLO, J. “La informática en la reforma de la Ley de Enjuiciamiento Criminal”, *Diario de La Ley*, núm. 8662, 2015. Pág. 6.

medida. El Ministerio Fiscal no tiene un papel activo en esta fase de ejecución de la medida, sino que figura como garante del respeto de los derechos fundamentales de las personas afectadas por la intervención¹⁸.

4.2.4. Duración de la medida.

La duración máxima inicial de la intervención es de **tres meses**, computada desde la fecha de autorización judicial, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses (art. 588 ter g LECrim).

La Policía Judicial podrá solicitar la prórroga de la medida, debiendo fundamentarle con la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida. El juez, antes de dictar resolución, podrá solicitar aclaraciones o mayor información, incluido el contenido íntegro de las conversaciones intervenidas (art. 588 ter h LECrim).

En cuanto a la prórroga, la STS 747/2017, de 21 de noviembre, FJ 7, indica que *“No tiene por qué reiterarse cada vez el marco general reflejado en los autos anteriores. Las prórrogas recaen en un contexto. Si había indicios y se razonó así ya y las escuchas no los han disipado, no es necesario en cada prórroga reproducir tediosa, repetitiva y cansinamente los indicios iniciales o los que han justificado cada nueva intervención. La sentencia de forma tan meritoria como elaborada y ordenada va reflejando la secuencia haciendo constar los informes policiales que daba lugar a cada nueva prórroga o ampliación”*.

4.2.5. Control de la intervención y el acceso de las partes a las grabaciones.

Como método de control de la medida de intervención, la Policía Judicial debe poner a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas, indicando su origen y destino, y asegurando, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas (art. 588 ter f LECrim).

¹⁸ RODRIGUEZ LAINZ, J.L. “La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014”, en *Diario La Ley*, núm. 8465, 2015. Pág. 18.

El TS se pronuncia al respecto del control de las intervenciones, estableciendo que *“durante la ejecución de la medida deberá existir un control judicial efectivo de la misma, para lo cual deberá el Juez tener puntual noticia del desarrollo de la misma y de los resultados que se vayan obteniendo. Al respecto debe distinguirse entre lo que puede constituir una posterior prueba (como son las grabaciones, sus transcripciones y la certificación de que éstas concuerdan con aquellas) y las actuaciones judiciales dirigidas a controlar la medida limitativa adoptada, pues en este caso -es decir, a los solos efectos de control- puede bastar con unas transcripciones que le permitan conocer la marcha de la intervención, sin perjuicio, de que si observara alguna circunstancia que exigiera un mayor control o un control más completo, el Juez debe proceder a oír las cintas grabadas o a examinar sus transcripciones debidamente certificadas”*¹⁹.

Mientras la intervención continúe vigente, *“Las deficiencias en el control o en la incorporación de las escuchas pueden efectivamente incidir en el derecho al secreto de las comunicaciones, máxime cuando se acuerda una prórroga o una nueva intervención, o ampliaciones basándose en anteriores escuchas no controladas”*²⁰.

Ahora bien, debemos aclarar qué se entiende por control judicial, ya que no es válido equipararlo con una mera audición o transcripción previa de todas las grabaciones por parte del Juez. Según el TS, *“Control judicial no significa inmediata audición de todas las grabaciones por el titular del juzgado. Para acordar la prórroga de una intervención telefónica no es necesario contar ya con la transcripción exacta de las previas conversaciones, sino tan solo con sus datos esenciales que pueden expresarse mediante un informe que sean justificativos de la procedencia de esa prolongación”*²¹.

En la misma línea, en la STC 26/2010, de 27 de abril, FJ 4, se estableció que *“Denuncia también la demandante la falta de control judicial en el seguimiento de la intervención. Al respecto, hemos afirmado que para dicho control no es necesario que la policía remita las transcripciones íntegras y las cintas originales y que el Juez proceda a la audición de las mismas antes de acordar prórrogas o nuevas intervenciones, sino que resulta suficiente el*

¹⁹ STS 938/2013, de 10 de diciembre, FJ 1.

²⁰ STS 747/2017, de 21 de noviembre, FJ 9.

²¹ Ídem.

conocimiento de los resultados obtenidos a través de las transcripciones de las conversaciones más relevantes y de los informes policiales... que sin lugar a dudas es lo que acontece en el presente supuesto, en el que, como ya se ha afirmado, el oficio policial en el que se solicita la prórroga, además de contener la información referida a los resultados de la investigación, se acompaña de las transcripciones de las conversaciones mantenidas en los teléfonos intervenidos. Por ello, puede afirmarse que por el órgano judicial se ha efectuado el pertinente seguimiento de la medida”.

Para finalizar con esta cuestión, como se indica en las STC 82/2002, de 22 de abril, FJ 6, resulta suficiente que quienes realicen materialmente las escuchas eleven al juez los informes y la exposición de las conversaciones más relevantes. No obstante, le instructor siempre podrá exigirles explicaciones, aclaraciones o correcciones.

En cuanto el control a posteriori, esto es, una vez finalizada la medida, el TS entiende que *“la finalización de la medida también exige un control respecto al material en el que se contienen las escuchas telefónicas realizadas. Esta custodia y guarda debe enmarcarse en el ámbito de la protección de las pruebas obtenidas, las cuales deben estar a disposición de las partes en el proceso penal”*²².

Respecto al acceso de las partes a las grabaciones, el art. 588 ter i LECrim establece que se entregará a las partes copia de las grabaciones y de las transcripciones realizadas cuando se alce el secreto y expire la vigencia de la medida de intervención. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos, debiendo hacerse constar expresamente tal exclusión de información. No obstante, una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa. El juez de instrucción notificará a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible,

²² Ídem.

exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. La persona notificada puede solicitar que se le entregue copia de la grabación transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

En relación a lo anterior, sobre la documentación e información de las partes respecto de la medida, dice la STS 107/2017, de 21 de enero, FJ 4: *"Los datos relevantes para la decisión sobre una intervención telefónica han de exteriorizarse y documentarse. No pueden completarse con otros que no pasan de conversaciones o comunicaciones, legítimas pero no formales, entre el Instructor y los agentes investigadores. Todo lo relevante para la intervención debe quedar plasmado en el oficio, en la causa (a través de una comparecencia en su caso en que consten las aclaraciones o datos complementarios alegados ante el Instructor) y en su caso en el auto (con las matizaciones derivadas de la posibilidad de heterointegración). Pero no cabe completar ex post la base indiciaria aduciendo que existían otros elementos que permanecieron ocultos frente a terceros, derivados de entrevistas entre los agentes y el instructor"*.

Como se aclaró en la STS 747/2017 de 21 noviembre, en su FJ 3, el instructor, como director de la investigación, puede recabar datos o aclaraciones verbalmente de los agentes o que éstos se las proporcionen, sin que exista ningún impedimento para ello. Ni tampoco existe ninguna prohibición para que se produzcan ese tipo de entrevistas o conversaciones dirigidas al esclarecimiento sobre algún punto de las informaciones obtenidas, siendo necesarias cuando de las comunicaciones orales se deriven datos relevantes o una orden significativa que adquieran la debida constancia. El TS entendió que no es necesario burocratizar la investigación, dejando todo documentado: *"Lo que sí será insoslayable en el momento de fiscalizar la legitimidad de las escuchas es estar en exclusiva a los datos obrantes en los autos. No pueden legitimarse unas escuchas basándose en supuestos conocimientos volcados en unas entrevistas cuyo contenido se oculta a las partes"*.

4.2.6. Valor probatorio de la medida.

Para concluir el estudio sobre la medida de interceptación de las comunicaciones telefónicas y telemáticas, es preciso indicar que, como indican al respecto el TS, *"las escuchas son prueba documental cuya reproducción en el juicio no debe ir precedida de las*

manifestaciones de quienes las llevaron a cabo. Son elementos objetivos. Las escuchas fueron objeto de transcripción en sede judicial, no impugnada, y las partes renunciaron a su audición”²³.

No es necesaria la valoración en el plenario de las escuchas. Dice a este respecto la STS 1029/2013, de 18 de diciembre, FJ 10:

“El reflejo documental de las escuchas (transcripciones) era prueba propuesta por el Ministerio Fiscal (folios 281 a 285 del rollo de Sala). Como también lo era la audición de las grabaciones (otrosí II de su escrito de conclusiones). Para la valorabilidad de las escuchas no es imprescindible su audición en el plenario. Menos, si ha sido renunciada por las partes. El art. 726 LECrim obliga al examen de las grabaciones propuestas como prueba y admitidas. Esa prescripción no rompe la esencialidad del principio de práctica de la prueba en el juicio oral. Tal postulado no implica que el Tribunal tenga que leer los documentos, o examinar las actuaciones a presencia de todas las partes y antes de concluir el juicio. La falta de lectura o audición en el acto del juicio oral carece de trascendencia. Fueron propuestas como prueba documental. Es claro -y lo es especialmente a partir de la sentencia del Tribunal Europeo de Derechos Humanos de 6 de diciembre de 1988 (Caso Barberá y otros) que la fórmula, rituarial y clásica en nuestro foro -"por reproducida"-, no convierte en prueba documental todas las actuaciones sumariales; ni transmuta en prueba documental lo que no son más que pruebas personales documentadas. La feliz recuperación de la importancia del acto del plenario como escenario idóneo para desplegar la actividad probatoria no puede llevar a instalarse en tesis radicales que, amén de insultar el sentido común, no suponen objetivamente ningún refuerzo de garantías procesales. La fórmula de "dar por reproducida" la prueba documental durante muchos años constituyó la coartada para obviar la esencialidad de la práctica de la prueba en el acto del juicio oral, con la consiguiente merma de los principios de publicidad, inmediación y contradicción. Ahora bien, la justa proscripción de esa corruptela contraria a los pilares básicos de la arquitectura del proceso penal que levantó el legislador del siglo XIX, no supone descalificar de manera absoluta ese mecanismo abreviado de práctica de la prueba documental. Que la prueba haya de practicarse en el acto del juicio oral, no significa que todos, absolutamente todos los documentos aportados o unidos a las actuaciones hayan de ser leídos en ese momento, so pena de quedar invalidados como posible medio de convicción. Eso

²³ STS 747/2017, de 21 de noviembre, FJ 11.

es absurdo y llevaría a la manejabilidad de determinados procesos penales en que la prueba es básicamente documental y además de un volumen ingente”.

La consideración respecto de que la reproducción en el acto de juicio oral de la integridad de las grabaciones no es obligada en ese escenario goza el refrendo del TC. Así, en la STC 26/2010, de 27 de abril, FJ 6, se dice: *“La audición de las cintas no es requisito imprescindible para su validez como prueba, sino que el contenido de las conversaciones puede ser incorporado al proceso bien a través de las declaraciones testimoniales de los funcionarios policiales que escucharon las conversaciones intervenidas, bien a través de su transcripción mecanográfica -como documentación de un acto sumarial previo... Y también hemos concluido que para dicha incorporación por vía documental no es requisito imprescindible la lectura de las transcripciones en el acto del juicio, siendo admisible que se dé por reproducida, siempre que dicha prueba se haya conformado con las debidas garantías y se haya podido someter a contradicción y que tal proceder, en suma, no conlleve una merma del derecho de defensa”.*

4.3.Incorporación al proceso de datos electrónicos de tráfico o asociados.

El art. 588 ter j LECrim, enmarcado en la Sección II del Capítulo V del Título VIII, establece la necesidad de una autorización judicial para la cesión de datos para su incorporación al proceso. Los datos a los que se refiere el citado artículo son los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación.

Cuando sea indispensable para la investigación el conocimiento de esos datos, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos. Para ello habrá que precisar la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

4.4. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

Por último, para finalizar la explicación del Capítulo V del Título VIII LECrim, en la Sección III se regula el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

4.4.1. Identificación mediante número IP.

En primer lugar, será necesario definir el concepto IP para poder abordar la identificación mediante número IP. Una dirección IP (acrónimo para Internet Protocol) es un número que sirve para identificar un dispositivo en una red²⁴. Está formada por un conjunto de cuatro números del 0 al 255, separados por puntos. En el art. 588 ter k LECrim se establece que cuando la Policía judicial, en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, conociera una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitará al juez de instrucción que requiera a los proveedores del servicio de información, en atención al deber de colaboración según el artículo 588 ter e, para que cedan los datos necesarios para la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso²⁵.

El TS señala que cualquier usuario puede acceder a la dirección IP, puesto que no se requiere una autorización judicial para conseguir lo que es público, ya que es el propio usuario de la red quien lo ha introducido en la misma. No obstante, si es necesario acudir al juez para que autorice el conocimiento de la identidad del dispositivo o el titular del contrato de una determinada dirección IP, a fin de garantizar el derecho a la intimidad personal (art. 18.1 CE)²⁶.

4.4.2. Identificación de los terminales mediante los códigos IMSI e IMEI.

Respecto a la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes, el art. 588 ter l LECrim permite a la Policía

²⁴ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 136.

²⁵ RUBIO ALAMILLO, J. *op. cit.* Pág. 8.

²⁶ SSTs 680/2010, de 14 de julio de 2010 y 739/2008, 12 de noviembre.

Judicial, sin necesidad de autorización judicial, acceder a los mismos cuando no sea posible obtener un determinado número de abonado que resulte indispensable a los fines de la investigación. Los códigos a los que hace referencia este artículo no son otros que la numeración IMSI²⁷ o IMEI²⁸. En otras palabras, la Policía Judicial, mediante barridos electrónicos sobre un determinado radio de acción podrá identificar el número del equipo de comunicación (IMSI) o el de la tarjeta para acceder a la red de telecomunicaciones (IMEI)²⁹.

Para mayor claridad, el IMSI es un número que identifica internacionalmente al usuario y a su operador, y que queda almacenado en la tarjeta SIM, sin estar impreso en su superficie. Por el contrario, IMEI es un número que identifica el dispositivo móvil, pero no tiene ninguna relación con el operador ni con la identidad del usuario. A partir del IMEI, el dispositivo móvil puede ser retirado de la red de forma rápida y sencilla, siendo muy útil para dejar inoperativo un teléfono en casos de sustracción del mismo³⁰.

Conforme a la jurisprudencia de Tribunal Supremo, queda extramuros del ámbito del secreto de las comunicaciones protegido constitucionalmente el conocimiento de los códigos IMSI o IMEI³¹. La concepción de comunicación protegida constitucionalmente *“comprende tanto la captura del número del abonado (si el acceso al servicio es por contrato), o del usuario (con el supuesto de tarjetas prepago que es el de esta causa) como la del código del terminal, que, por una vía más indirecta, permite obtener el mismo efecto de invasión del ámbito del secreto”*³². No obstante, según la doctrina del TEDH, deben distinguirse los números marcados en el teléfono de la numeración IMSI asociada a un teléfono móvil, en tanto que dicho código no contiene el número concreto del teléfono móvil, ni el del usuario y el sistema del *comptage* referido al listado de llamadas entrantes y salientes efectuadas desde un teléfono móvil.

²⁷ International Mobile Subscriber Identity (Identidad Internacional del abonado a un móvil).

²⁸ International Mobile Station Equipment Identity (Identidad internacional de equipo móvil).

²⁹ JIMENEZ SEGADO, C. y PUCHOL AIGUABELLA, M. “Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección de datos”, en *Diario La Ley*, núm. 8676, 2016. Pág. 7.

³⁰ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 135.

³¹ SSTs 55/2007, de 23 de enero, FJ 1; 686/2013, de 29 de julio, FJ 3.

³² STS 130/2007, de 19 de febrero, FJ 1.

Podemos afirmar que este listado puede incidir en la intimidad de las personas, aunque el nivel de injerencia será menor que la interceptación de una conversación³³.

Obtenidos los códigos citados anteriormente, la Policía Judicial puede solicitar al Juez la intervención de las comunicaciones conforme al artículo 588 ter d LECrim.

Cabe aquí hacer referencia al acceso a la agenda de los teléfonos móviles, entendiendo el TS que no se trata de una intromisión en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad³⁴, por lo que debe aplicarse la doctrina del TC sobre la limitación de dicho derecho con motivo de las investigaciones delictivas por los agentes policiales³⁵. Por agenda se entiende el archivo del dispositivo en el que consta un listado de números identificados normalmente por un nombre, equiparándose a una agenda electrónica o en soporte papel. Su registro no interfiere en el derecho al secreto de las comunicaciones, sino en la intimidad³⁶.

4.4.3. Identificación de titulares o terminales o dispositivos de conectividad.

Por último, el art. 588 ter m LECrim trata la identificación de los titulares o terminales o dispositivos de conectividad, disponiendo que cuando el Ministerio Fiscal o la Policía Judicial, en el ejercicio de sus funciones, precisen de conocer los aspectos indicados, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia. Este precepto permite proceder *motu proprio* al Ministerio Fiscal y a la Policía Judicial para obtener los datos necesarios que los sujetos obligados tienen el deber de proporcionar.

En relación a lo anterior, el Acuerdo del Pleno de la Sala 2ª del TS de 23 de febrero de 2010 acordó que “*es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el MF precisará de tal autorización para*

³³ STS 686/2013, de 29 de julio, FJ 3.

³⁴ STS 663/2011, de 7 de julio.

³⁵ STC 120/2002, de 20 de mayo.

³⁶ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 137.

obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre”³⁷.

4.5.La interceptación de las comunicaciones de WhatsApp.

Desde el año 2009, WhatsApp ha ido ganando usuarios en España. A día de hoy, prácticamente todos lo utilizamos, habiendo revolucionado los hábitos de la población, que ha dejado de utilizar el método tradicional de SMS para interaccionar con sus conocidos, cambiándolo por la mensajería instantánea que funciona mediante la conexión a Internet. No obstante, a pesar de sus numerosas ventajas, también se ha destinado a malos usos y se ha convertido en una herramienta más a través de la que cometer “cibercrímenes”.

La interceptación de las comunicaciones de WhatsApp constituye una diligencia de investigación en el proceso penal bajo el amparo legal de la reciente reforma de la LECrim. Por la naturaleza de esta aplicación de mensajería instantánea, se sitúa bajo la rúbrica de los Capítulos IV y V del Título VIII del Libro II de la LECrim. Pero para que este tipo de intervención esté justificada deberá observar estrictamente los requisitos legales, tanto los comunes exigidos para cualquier intervención tecnológica, como los específicos para la intervención de una comunicación telefónica y telemática.

El primero de los presupuestos que debe concurrir para interceptar las conversaciones de WhatsApp entre dos o más usuarios es que medie autorización judicial previa. No obstante, en casos de urgencia y en que se estén investigando delitos relacionados con la actuación de bandas terroristas y existan razones fundadas que hagan imprescindible la medida, podrá ser adoptada sin autorización judicial previa, pero deberá ser confirmada y superar ese filtro posteriormente. En circunstancias normales, el Juez podrá autorizar la medida de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. Si seguimos lo establecido en el art. 588 bis b LECrim, la acusación particular o popular no tendrían legitimación para solicitar la intervención de las comunicaciones de WhatsApp mantenidas por el investigado. Dicho precepto parece oponer a lo dispuesto en el art. 311.1 LECrim, que prevé que *“El juez que instruya el sumario practicará las diligencias que le propusieren el Ministerio Fiscal o cualquiera de las partes personadas, si no las considera inútiles o perjudiciales”*.

³⁷ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *op. cit.* Pág. 136.

Respecto a los requisitos específicos para poder intervenir las comunicaciones del investigado a través de WhatsApp, como dicta el art. 588 ter a LECrim, la medida solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. En definitiva, la cuestión versa sobre la limitación del derecho al secreto de comunicaciones teniendo en cuenta bien la entidad de la conducta delictiva objeto de investigación penal, o bien atendiendo a la forma en la que aquélla hubiera sido cometida.

Por consiguiente, podemos observar que la Ley ha ampliado el ámbito material de esta medida de investigación con respecto a la intervención de las comunicaciones escritas y telegráficas. En estos casos, será muy importante tener en cuenta los principios de proporcionalidad y excepcionalidad a fin de no autorizar la intervención cuando los delitos perseguidos no tengan mucha trascendencia.

Por otro lado, fuera de los supuestos en que las conversaciones de WhatsApp son intervenidas por las autoridades, encontramos el supuesto en que las propias partes en el proceso pretenden hacer valer el contenido de dichas conversaciones en el proceso penal como fuente de prueba, bien en la fase de instrucción, bien en el juicio oral.

La LECrim no prevé expresamente como introducir pruebas de la naturaleza que tiene una conversación de WhatsApp, la cual no se haya en un soporte material o físico, sino que es virtual. Pero no parece que exista ningún impedimento para aportar al Juez el propio terminal donde se encuentra la conversación, además de entregar una transcripción de los mensajes en soporte papel, lo cual hace que se aplique el mismo tratamiento que a la prueba documental. Podría tratarse de la constitución de un documento privado o público, si se solicita a un notario que eleve acta del contenido de las conversaciones de WhatsApp. Durante el proceso, también puede presentarse la prueba mediante el interrogatorio de las partes o mediante un dictamen pericial sobre el contenido de la conversación.

Otro problema que surge respecto a esta cuestión es la valoración de la prueba de WhatsApp.

Conforme al art. 741 LECrim *“El Tribunal, apreciando, según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo*

manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley”. Pues bien, dicho precepto establece la libertad del juzgador a la hora de discernir qué pruebas tendrán eficacia probatoria en el proceso, siguiendo los principios de razonabilidad, no arbitrariedad y motivación.

En la valoración de la prueba de WhatsApp, la controversia se suscita cuando la conversación es impugnada por alguna parte, en tanto que es fácilmente manipulable, pudiendo ser borradas algunas partes de la conversación o simularla una conversación falsa. En estos casos, el Juez deberá tener especial cuidado al realizar la valoración de la prueba.

Según la STS 300/2015, de 19 de mayo, FJ 4, *“La prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo*”. A continuación, fija el criterio sobre a quien corresponde la carga de la prueba en caso de la aportación de documentos impresos: *“De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*”.

Para finalizar, como hemos observado, esta corriente jurisprudencial exige a quien aporta una conversación de WhatsApp que ha sido impugnada la aportación de un informe pericial que compruebe la veracidad de la conversación, la identidad de los sujetos intervinientes y su contenido.

4.6. Supuestos controvertidos de intervención de las comunicaciones.

Uno de los supuestos más controvertidos respecto a la intervención y grabación de las comunicaciones orales es el de las **conversaciones entre abogado y cliente**.

Cabe recordar que uno de los fines de la LO 13/2015 se trata de la transposición a de la Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre

el derecho a la asistencia de letrado en los procesos penales. El art. 4 de la Directiva dispone la obligación de respetar la confidencialidad de las comunicaciones entre los investigados y sus letrados, haciendo referencia expresa a reuniones, correspondencia, conversaciones telefónicas y cualesquiera otras formas de comunicación que pudieran ser intervenidas. Sin embargo, en la Exposición de Motivos de la LO 13/2015 se indica que el derecho al secreto de las comunicaciones entre el investigado y su abogado puede ser restringido si se dan ciertas circunstancias, tales como la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado.

El art. 118.4 LECrim establece que *“Todas las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial. Si estas conversaciones o comunicaciones hubieran sido captadas o intervenidas durante la ejecución de alguna de las diligencias reguladas en esta ley, el juez ordenará la eliminación de la grabación o la entrega al destinatario de la correspondencia detenida, dejando constancia de estas circunstancias en las actuaciones. Lo dispuesto en el párrafo primero no será de aplicación cuando se constate la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal, sin perjuicio de lo dispuesto en la Ley General Penitenciaria”*.

De la regulación anteriormente expuesta podemos concluir que las comunicaciones telefónicas entre el investigado y su abogado pueden ser interceptadas y grabadas, en los supuestos en que haya indicios de actividad delictiva en relación con alguno de los delitos que determina el artículo 558 bis a) LECrim; con la única salvedad de que deberán ser excluidas del procedimiento aquellas grabaciones que afecten al derecho de defensa del cliente y carezcan de relación alguna con la actividad delictiva investigada.

Por otro lado, se plantea la duda de si pueden grabarse las **conversaciones telefónicas propias**. A este respecto, la STS 239/2010, de 24 de marzo, FJ 3, indica que *“Es reiterada jurisprudencia del TC, seguida por el TS e iniciada por la sentencia del TC núm. 114/1984 de 29 de noviembre, la que establece que el derecho al secreto de las comunicaciones salvo resolución judicial no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida. [...] Sea cual sea el ámbito objetivo del concepto de “comunicación”, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia “erga*

omnes”) ajenos a la comunicación misma. [...] No hay “secreto” para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el art. 18.3 CE la retención, por cualquier medio, del contenido del mensaje. [...] Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera “intima” del interlocutor, pudiesen constituir atentados al derecho garantizado en el art. 18.1 CE. Otro tanto cabe decir, en el presente caso, respecto de la grabación por uno de los interlocutores de la conversación telefónica. Este acto no conculca secreto alguno impuesto por el art. 18.3”.

Conforme a lo anterior, podemos afirmar que el art. 18.3 CE se encarga de la protección del derecho al secreto de las comunicaciones, garantizando que no haya injerencias por terceras personas ajenas a la comunicación. Para los partícipes en la comunicación no existe secreto, sin que se encuentren bajo la limitación constitucional, pudiendo disponer del contenido de la comunicación con total libertad sin afectar al derecho fundamental.

No resulta contrario a la jurisprudencia que la conversación sea grabada por un tercero, con el consentimiento de alguno de los participantes en ella,

Esta doctrina jurisprudencial no se ve afectada por la circunstancia de que sea un tercero quien, con el consentimiento de uno de los interlocutores, grabe la conversación, tal y como se señala en la STS 298/2013, de 13 de marzo, FJ 1: *“La utilizabilidad de ese medio de prueba no queda supeditada a la conformidad en la grabación de todos los partícipes o contertulios; ni a la ausencia de toda connotación subrepticia o de engaño u ocultación por parte de quien dispone lo necesario para la fijación en un soporte de la conversación. Es suficiente que uno de los comunicantes o interlocutores preste su consentimiento para la intervención y grabación por un tercero para que resulte inoperante la cláusula de exclusión del art. 11 LOPJ. Es un elemento probatorio valorable. Sólo la escucha o grabación por un tercero sin autorización de ninguno de los comunicantes ni de la autoridad judicial convierte en inutilizable ese medio probatorio”.*

Otro supuesto es el de la intervención de las **comunicaciones orales emitidas por radiofrecuencia**. La intervención de las comunicaciones por radio no necesita autorización judicial, ya que no queda bajo la rúbrica del secreto del art. 18.3 porque son públicas. El alcance

del secreto a las comunicaciones se limita a las conversaciones privadas o reservadas. Es por ello que, en el caso de la radio, no es exigible una autorización judicial para acceder al contenido de ese tipo de comunicaciones porque ya son públicas en sí mismas.

En este sentido, reiterada jurisprudencia del TS ha apoyado el carácter público de las comunicaciones radiotelegráficas. La STS 695/2013, de 22 de julio, FJ 12, señala que *“Como decíamos en la STS 1397/2011 de 22 de diciembre, con citación de la STS 209/2007, de 9 de marzo, y en un supuesto muy similar al de autos, donde dicha captación tiene lugar, también en el curso de otra investigación, las captaciones de conversaciones radiotelegráficas, en frecuencia de uso público, no precisan autorización judicial, porque precisamente por ser de uso público y siendo esto conocido por los usuarios, ello implica una implícita aceptación de la posibilidad de captación”*.

5. RÉGIMEN JURÍDICO DE LA CAPTACIÓN Y GRABACIÓN DE COMUNICACIONES ORALES MEDIANTE LA UTILIZACIÓN DE DISPOSITIVOS ELECTRÓNICOS.

La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos es regulado por el Capítulo VI del Título VIII del Libro II de la LECrim, también introducido en el artículo único, apartado quince, de la Ley Orgánica 13/2015.

La necesidad de dar una cobertura legal a este tipo e intervención de las comunicaciones orales ya fue detectada por el TC con anterioridad a la reforma de la LECrim. En la STC 145/2014, de 22 de septiembre, el demandante denunciaba la vulneración de vulnerado su derecho al secreto de las comunicaciones (art. 18.3 CE) por falta de garantías constitucionales en las escuchas telefónicas que fueron practicadas y por la grabación de las conversaciones que tuvieron lugar en los calabozos y en dependencias policiales³⁸. El TC resolvió que dichas escuchas no tenían amparo legislativo por carecer de cobertura legal³⁹. Ésta había sido doctrina constante del TC, en cuanto a las garantías del derecho fundamental del derecho al secreto de las comunicaciones, indicando que *“por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal”*⁴⁰.

El preámbulo de la reforma se pronuncia al respecto de esta cuestión, postulando que *“la experiencia demuestra que, en la investigación de determinados delitos, la captación y grabación de comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos puede resultar indispensable. Se trata de una materia hasta ahora ausente de la regulación del proceso penal y cuyo alcance se aborda con sujeción a dos ideas clave. La primera, la exigencia de que sea el juez de instrucción el que legitime el acto de injerencia; la segunda, la necesidad de que los principios rectores de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad actúen como elementos de justificación de la medida. Esta medida solo podrá acordarse para encuentros concretos que vaya a mantener el investigado,*

³⁸ STC 145/2014, de 22 de septiembre, FJ 1.

³⁹ Ídem, FJ 6 y 7.

⁴⁰ STC 49/1999, de 5 de abril, FJ 3.

debiéndose identificar con precisión el lugar o dependencias sometidos a vigilancia. Por tanto, no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas, y, en consecuencia, el dispositivo de escucha y, en su caso, las cámaras a él asociadas, deberán desactivarse tan pronto finalice la conversación cuya captación fue permitida, como se desprende del artículo 588 quater c”.

A continuación, expondremos la regulación de las cuestiones tratadas anteriormente que introduce la nueva redacción de nuestra norma procesal.

5.1. Grabación de las comunicaciones orales directas.

En la STS 297/2017, de 26 de abril, FJ 4, el recurrente denunciaba la vulneración del derecho a la presunción de inocencia con respecto a la prueba de grabación de conversaciones ambientales, en relación con las escuchas realizadas mediante un dispositivo colocado en el vehículo de uno de los condenados. El TS resolvió indicando que *“En cuanto al criterio para la determinación de la validez de las grabaciones ambientales de conversaciones directas entre dos o más personas, hemos de remitirnos a la doctrina de esta Sala y del Tribunal Constitucional coincidente con la citada por el recurrente. Efectivamente la grabación o intervención de comunicaciones presenciales directas entre dos o más personas no encuentra habilitación legal en el texto del anterior artículo 579 de la LECrim”.*

Con la nueva regulación introducida por la LO 13/2015, el art. 588 quater a LECrim autoriza, por primera vez, a la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados. Dichos dispositivos pueden colocarse tanto en el interior como en el exterior del domicilio o lugar cerrado.

En este caso no importa si la grabación es obtenida desde el exterior del espacio cerrado donde el investigado mantiene las comunicaciones, y sin acceder al mismo. No se hace énfasis sobre el medio técnico utilizado para practicar las grabaciones sino en el derecho fundamental afectado, es decir, el secreto a las comunicaciones (art. 18.3 CE).

Será necesaria una resolución judicial motivada para acceder a alguno de los lugares citados anteriormente o todos aquellos destinados al ejercicio de la privacidad.

Las grabaciones de las comunicaciones orales que se tratan en este precepto pueden ser complementadas con la obtención de imágenes, si así lo autoriza expresamente la resolución judicial que acuerde la medida.

Hoy en día, los teléfonos móviles o smartphones han alcanzado un desarrollo técnico muy avanzado, lo que permite que sean utilizados como micrófonos. De este modo, el uso del teléfono como medio de investigación criminal quedaría bajo la rúbrica de captación y grabación de las comunicaciones orales directas mediante la utilización de dispositivos electrónicos.

5.2.Presupuestos.

En relación a los presupuestos necesarios para la autorización de la medida, en primer lugar, la utilización de los dispositivos a que se refiere el artículo anterior debe estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación.

Enumera el art. 588 quater b que la medida sólo podrá ser autorizada cuando concurren los requisitos siguientes:

- a) Que los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos:
 - 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
 - 2.º Delitos cometidos en el seno de un grupo u organización criminal.
 - 3.º Delitos de terrorismo.
- b) Que pueda racionalmente preverse que la utilización de los dispositivos aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor.

Nos encontramos, pues, con los mismos requisitos que exige el art. 579.1 LECrim para autorizar la detención de la correspondencia escrita o telegráfica.

Respecto al primer supuesto de limitación, delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, se han pronunciado el TS y el TC. Consideran que la intervención de las comunicaciones orales se trata de una medida invasiva que afecta gravemente a la intimidad de las personas, por lo que debe tenerse en cuenta, con motivo de su autorización, la gravedad de la infracción objeto de la investigación. Tal gravedad no se mide exclusivamente por la gravedad de la pena atribuida por el Código Penal a la conducta investigada, “aunque la pena no sea calificada de grave por el Código penal, la infracción puede serlo en atención a la consideración de otros criterios como la importancia del bien jurídico protegido o la relevancia social de los hechos”⁴¹.

El Tribunal Supremo, en su sentencia 938/2013, de 10 de diciembre, FJ 1, indicaba que: *“respecto a la proporcionalidad de la medida injerente, es doctrina de esta Sala y del Tribunal Constitucional la que señala que ha de ser medida en función de la gravedad de la infracción objeto de la investigación y esta no se mide, exclusivamente, por la gravedad de la pena que a la conducta investigada anuda el Código penal, por más que es un criterio relevante, incluso en muchos casos determinante para medir esa gravedad que autoriza la injerencia en el derecho fundamental”*.

5.3.Contenido de la resolución judicial.

La resolución judicial que autorice la medida, además de los requisitos genéricos del art. 588 bis c LECrim, deberá contener una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia (art. 588 quater c LECrim).

Esta última exigencia es una de las novedades introducidas por la Ley 13/2015, una vez, persiguiendo dotar a la resolución judicial que autorice la medida de un sentido garantista.

5.4.Control de la medida.

Cumpliendo con las exigencias del art. 588 bis g LECrim, la Policía Judicial pondrá a disposición de la autoridad judicial el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones

⁴¹ SSTs 343/2012, de 30 de abril; 503/2013, de 19 de junio; 938/2013, de 10 de diciembre; SSTC 299/2001, de 11 de diciembre; 14/2001, de 29 de enero.

que considere de interés. El informe identificará a todos los agentes que hayan participado en la ejecución y seguimiento de la medida (art. 588 quater d LECrim).

5.5.Cese.

En primer lugar, debemos recordar la importancia de la duración de la medida, en tanto que se trata de una diligencia de investigación que hace una injerencia en los derechos fundamentales del investigado, pudiendo vulnerarlos. Conforme al art. 588 bis e LECrim, con carácter general, y si la regulación específica de la medida no establece un plazo concreto, la duración de la medida no podrá exceder del tiempo imprescindible para el esclarecimiento de los hechos. En el Capítulo VI, el cual nos ocupa este apartado, no existe ninguna referencia a la duración de la medida. Se trata de un vacío que, bajo nuestro punto de vista, debería ser regulado por el legislador estableciendo un plazo concreto de duración máxima de la medida y el establecimiento del cómputo inicial y final del mismo. De lo contrario, la intervención las comunicaciones orales podría convertirse en una medida propia de un Estado de policía, abusiva en un sistema democrático de Derecho⁴².

Respecto al cese de la medida, el art. 588 quater d LECrim establece que, cesada la ésta por alguna de las causas previstas en el artículo 588 bis j, la grabación de conversaciones que puedan tener lugar en otros encuentros o la captación de imágenes de tales momentos exigirán una nueva autorización judicial.

5.6.Casos susceptibles de grabación de las comunicaciones orales.

5.6.1. Utilización de micrófonos.

Ha sido generalizado en numerosos países el uso de micrófonos de ambiente para grabar las conversaciones mantenidas por los sujetos investigados por la comisión de algún delito grave. Sobre ello se ha pronunciado en numerosas ocasiones el TEDH, concluyendo que la captación secreta de conversaciones o imágenes por medio de aparatos de grabación de audio y vídeo entraba en el campo de aplicación del artículo 8 del Convenio, tanto en lo referente al derecho al respeto de la vida privada como de la correspondencia. Lo ha hecho, por ejemplo, en la colocación y utilización de aparatos de escucha en una celda de un detenido en prisión

⁴² CASANOVA MARTÍ, R. “La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos”, en *Diario La Ley*, núm. 8674, 2016. Pág. 6.

(STEDH de 25.9.2001, P.G y J.H. contra Reino Unido); en el establecimiento de un dispositivo de vigilancia de audio y vídeo colocado en la celda de un detenido en prisión y en la zona de visita de esta (STEDH. 5.11.02), (Allan contra Reino Unido); y a la grabación y conversaciones telefónicas de un preso por las autoridades penitenciarias, utilizadas posteriormente como elemento de prueba para condenarle por otro delito (STEDH. 27.4.2004, Doerga contra Holanda)⁴³.

En nuestro país, el TS vino admitiendo la doctrina expuesta sin más exigencia que la existencia de una autorización judicial que concediera la utilización de esta técnica de investigación. Sin embargo, en contraposición, el TC cuestionó esta posición en la STC 145/2014, de 22 de septiembre, FJ 7, otorgando el amparo solicitado y estimando que la grabación realizada sobre las comunicaciones del detenido en las celdas policiales había vulnerado el derecho al secreto de las comunicaciones del recurrente. Tales grabaciones habían sido autorizadas mediante auto motivado del Juzgado de Instrucción, en base al art. 579.2 LECrim, remarcando el TC que la necesidad de la previa habilitación legal para la legalidad de cualquier injerencia en los derechos fundamentales: *“Aunque la literalidad de dicho precepto (“se garantiza el secreto de las comunicaciones y, en especial, las postales, telegráficas y telefónicas, salvo resolución judicial”) puede inducir a pensar que la única garantía que establece inmediatamente la Constitución es la exigencia de autorización judicial, un análisis más detenido de la cuestión pone de manifiesto lo contrario, ya que, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal. Esa misma jurisprudencia dispone que la reserva de ley constituye “el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas”, lo que “implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate”, pero que en todo caso determinan que “el legislador ha de hacer el ‘máximo esfuerzo posible’ para garantizar la seguridad jurídica”, esto es, “la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho” (STC 49/1999, FJ 4). Profundizando en esa exigencia,*

⁴³ CORTÉS LÓPEZ, M.J., “Grabación de Conversaciones y Secreto de las Comunicaciones: Estudio de la sentencia del Tribunal Constitucional de fecha 22 de Septiembre de 2014”, en *Revista de Derecho vLex*, núm. 132. Mayo 2015.

en la STC 169/2001, 16 de julio, FJ 6, sostuvimos, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias, que “la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad”.

En la actualidad, tras la entrada en vigor de la LO 13/2015, ya no existen dudas en torno a la legalidad de la medida de grabación de las comunicaciones orales directas de los investigados, siempre que se cumplan con las previsiones legales al respecto.

5.6.2. Utilización de cámaras ocultas.

El uso de cámaras ocultas afecta al derecho a la intimidad del sujeto afectado por la misma (art. 18.1 CE). Si la grabación es utilizada en el contexto de una investigación criminal nos encontraríamos ante un conflicto de intereses entre el derecho a la intimidad y el objetivo de la medida de investigación, el cual debe ser resuelto mediante la aplicación del juicio de proporcionalidad, necesidad y racionalidad.

Así lo señala la STS 793/2013, de 28 de octubre, FJ 2, *“la conclusión acerca de la licitud o exclusión de esa prueba sólo puede ser el desenlace lógico de un riguroso juicio de ponderación entre los derechos a la intimidad y a la propia imagen y la posible existencia de un fin legítimo, atendiendo siempre a los principios de proporcionalidad, necesidad y racionalidad. Sólo entonces, después de hacer explícitas las razones y criterios que han presidido la tarea ponderativa, se estará en condiciones de proclamar la legitimidad del sacrificio de aquellos derechos o, por el contrario, su exclusión como fuente de prueba por su irreparable ilicitud. Son perfectamente imaginables supuestos en los que esas imágenes, por su propio contenido, por el lugar en el que han sido captadas, por el contexto en el que se ha desarrollado la entrevista, por el papel asumido por sus protagonistas y, en fin, por la escasa gravedad del hecho cuya prueba se pretende garantizar, puedan justificar su rechazo. Sin embargo, no faltarán otros en los que el examen en el proceso penal de esas imágenes grabadas, con el consiguiente sacrificio del derecho a la intimidad del interlocutor, estará más que justificado. Optar por una u otra solución y motivar las razones que explican la decisión jurisdiccional es una exigencia de nuestro sistema constitucional”.*

Como ya hemos visto, el art. 588 quinquies a LECrim permite a la Policía Judicial, sin necesidad de autorización judicial previa, obtener y grabar imágenes de cualquier persona investigada que se encuentre en lugares públicos, cuando ello fuere necesario a los fines de la investigación o para el esclarecimiento de los hechos o localización de efectos o instrumentos del delito. Dicho precepto autoriza exclusivamente a la captación de la imagen, pero no a la del sonido, lo cual es una cuestión que queda situada dentro del ámbito del art. 588 quater a LECrim. Este precepto, tras regular la captación y grabación de sonido previa autorización judicial, añade que la escucha y grabación de las conversaciones privadas podrá complementarse con la grabación de imágenes cuando expresamente lo acuerde la resolución judicial habilitante. Por tanto, la Policía Judicial necesitará autorización judicial para la grabación del sonido junto con la imagen en lugares públicos, estando únicamente exenta de esa autorización previa la grabación de imágenes videográficas sin sonido.

6. RÉGIMEN JURÍDICO DE LA UTILIZACIÓN DE DISPOSITIVOS TÉCNICOS DE CAPTACIÓN DE LA IMAGEN, DE SEGUIMIENTO Y DE LOCALIZACIÓN.

La utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización se encuentra regulada en el Capítulo VII del Título VIII del Libro II de la LECrim, introducido en el artículo único, apartado dieciséis, de la Ley Orgánica 13/2015.

Esa medida tiene dos vertientes, que abordaremos a continuación: por un lado, la captación de imágenes en lugares o espacios públicos, y, por otro lado, la utilización de dispositivos o medios técnicos de seguimiento y localización.

6.1.Captación de imágenes en lugares o espacios públicos.

El art. 588 quinquies a LECrim faculta a la Policía Judicial a obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

Debemos distinguir esta medida de investigación de la regulada por el art. 588 quater a LECrim, que regulaba los presupuestos que permiten la captación de comunicaciones en el domicilio del investigado o en recintos cerrados, mientras que el artículo que nos ocupa este apartado se refiere a espacios públicos. Podemos observar que el escenario en el que se desarrolla la medida es distinto y, en consecuencia, el nivel de injerencia en la intimidad del investigado es inferior, así como en los derechos fundamentales afectados. Es por ello que para la captación de imágenes en lugares públicos no se precisa autorización judicial, sino que es la propia Policía Judicial la que puede tomarla por propia iniciativa.

En cuanto al ámbito subjetivo de la medida, ésta podrá afectar no sólo al investigado, sino a personas distintas del mismo, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.

6.2.Utilización de dispositivos o medios técnicos de seguimiento y localización.

Esta diligencia de investigación está regulada en el art. 588 quinquies b y c LECrim. A diferencia de lo que prevé la norma en el caso anterior, para la utilización de estos dispositivos

de seguimiento y localización sí se requiere una autorización judicial previa, siempre que queden acreditadas las razones que la justifican y la medida resulte proporcionada. De nuevo el legislador ha introducido el criterio de necesidad y proporcionalidad de la medida, como garantía de la posible afectación de los derechos fundamentales. Por ello, obliga a que el juez especifique en la autorización el medio técnico que va a ser utilizado.

No obstante lo anterior, cuando concurren razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, podrá exceptuarse la exigencia de autorización judicial. En estos casos, la Policía Judicial estará facultada para proceder a la colocación de dichos dispositivos. A continuación, en el plazo máximo de veinticuatro horas, deberá dar cuenta a la autoridad judicial para que ratifique la medida adoptada o acuerde su inmediato cese, en el mismo plazo. En el supuesto de cese de la medida, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso.

En cuanto a la duración inicial, la medida no podrá superar un periodo de tres meses a partir de la fecha de su autorización. Se contempla la posibilidad excepcional de que el juez acuerde prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida.

Una vez finalizadas las investigaciones, así como cuando el juez lo solicite, la Policía Judicial deberá entregarle los soportes originales o copias electrónicas auténticas que contengan la información recogida. Dicha información deberá ser debidamente custodiada para evitar su utilización indebida.

Por último, se vuelve a hacer referencia al deber de colaboración *ex art. 588 ter e LECrim*, estando obligados los prestadores, agentes y demás personas incluidas en el citado precepto a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia.

7. RÉGIMEN JURÍDICO DEL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN.

El registro de dispositivos de almacenamiento masivo de información se regula en el Capítulo VIII del Título VIII del Libro II de la LECrim, introducido en el artículo único, apartado diecisiete, de la Ley Orgánica 13/2015.

En primer lugar, y antes de abordar el fondo de la cuestión, debemos definir qué se entiende por dispositivos de almacenamiento masivo de información. Los preceptos que desarrollan la medida que nos ocupa hacen referencia a la aprehensión y acceso al contenido de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos (arts. 588 sexies a, b y c LECrim). El Tribunal Supremo entiende que éstos “*incluyen los instrumentos de comunicación telefónica, y, en consecuencia, los terminales de telefonía móvil*”⁴⁴.

Según DELGADO MARTÍN, los dispositivos de almacenamiento masivo de información tienen como nota común la utilización de un lenguaje binario mediante un sistema que permite transformar impulsos eléctricos o fotosensibles, y que genera y almacena la información a través de su descomposición y recomposición informática grabada en formato electrónico. Este tipo de prueba electrónica se diferencia de otras pruebas en que el lenguaje utilizado es un código informático que debe ser traducido al lenguaje alfabético común⁴⁵.

En otras palabras, se trata de cualquier dispositivo electromecánico o electrónico, capaz de guardar a largo plazo información generada por los usuarios, sin importar su origen u objetivos de tales datos. Podemos encontrar una amplia gama de dispositivos destinados a tal fin, los cuales pueden ser clasificados conforme a sus principios de almacenamiento: mecánicos, magnéticos, digitales, ópticos y mixtos⁴⁶.

⁴⁴ STS 204/2016, de 10 de marzo de 2016, FJ 11.

⁴⁵ DELGADO MARTÍN, J., “Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015”, en *Diario La Ley*, núm. 8693, 2016. Pág. 2-3.

⁴⁶ Dispositivos de almacenamiento masivo (en línea), http://www.informaticamoderna.com/Disp_almacen.htm (consulta 10 de abril de 2018).

- Dispositivos de almacenamiento mecánico: su almacenamiento está basado en elementos táctiles y visibles al ser humano (surcos y orificios), tales como tarjetas perforadas y discos musicales de vinilo.
- Dispositivos de almacenamiento magnético: basan su almacenamiento en partículas magnéticas microscópicas almacenadas bajo una capa de pintura especial en cintas de respaldo, disquetes, discos ZIP y discos duros.
- Dispositivos de almacenamiento óptico: su almacenamiento se basa en pequeñas ranuras microscópicas grabadas por medio de un láser en la superficie de un disco plástico, tales como CD-ROM, DVD-ROM, HD-DVD y Disco Blu-Ray.
- Dispositivos de almacenamiento electrónico-digital: a diferencia de los anteriores, basan su almacenamiento en celdas de memoria, sin ningún tipo de elementos mecánicos internos que generen desgaste. Se subdividen en dos tipos:
 - Almacenamiento temporal: la información es guardada por un periodo corto de tiempo (memorias RAM o SRAM).
 - Almacenamiento a largo plazo: guardan la información por periodo indefinido siempre y cuando el dispositivo no se dañe (USB, memorias ROM, chips de teléfono móvil y memorias digitales).
- Dispositivos de almacenamiento mixtos: combinan las tecnologías anteriores.

La problemática que se suscita respecto a los dispositivos señalados es la determinación de qué derecho se ve afectado, en atención a la información que se contiene en ellos: derecho a la intimidad (art. 18.1 CE), derecho al secreto de las comunicaciones (art. 18.3 CE) o derecho a la protección de datos (art. 18.4 CE). La jurisprudencia del TC no es clara al respecto, dando respuestas contradictorias para la cuestión⁴⁷.

Aclarada ya la noción de dispositivos de almacenamiento masivo de información, vamos a exponer a continuación los requisitos para la práctica de la medida que nos ocupa este apartado.

⁴⁷ GONZÁLEZ-CUELLAR SERRANO, N. y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015. Pág. 371.

7.1.Ámbito de la medida.

La rúbrica del Capítulo VIII del Título VIII de la LECrim se refiere al “*Registro de dispositivos de almacenamiento masivo de información*”. El articulado que desarrolla la regulación de la medida (arts. 588 sexies a, b y c LECrim) se refiere al acceso y aprehensión de *ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital y repositorios telemáticos de datos*.

En un sentido estricto, se consideran dispositivos de almacenamiento masivo de información los instrumentos informáticos destinados a guardar o registrar información del usuario a largo plazo. No obstante, la regulación de la medida no debe dirigirse solamente a aquellos dispositivos, descritos desde un punto de vista estricto, sino que debe aplicarse también al acceso de cualquier tipo de dispositivo electrónico destinado a guardar información, aunque sea de forma temporal y secundaria a las funciones que constituyen su objetivo primario, como sería el caso de los teléfonos móviles o *tablets*. En consecuencia, cualquier dispositivo tecnológico que, sin ser propiamente un dispositivo de almacenamiento masivo, pueda almacenar datos de los que obtener pruebas electrónicas respecto a la actividad delictiva puede ser objeto material de esta medida⁴⁸.

7.2.Necesidad de motivación individualizada.

El art. 588 sexies a LECrim regula lo que denomina la necesidad de motivación individualizada. Establece que cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos. De este precepto se hace notable la insuficiencia de una autorización que se limite a la entrada y registro en el domicilio del sujeto investigado para poder acceder a la información que guardan los dispositivos electrónicos que se hallen el mismo, puesto que la policía no está facultada para ello, sino que el auto deberá pronunciarse expresa y motivadamente en cada caso.

⁴⁸ MARTÍN MARTÍN DE LA ESCALERA, A.M., *op. cit.* Pág. 5.

Puede suceder que en la práctica de un registro domiciliario se encuentren dispositivos de almacenamiento masivo de información, pero la simple incautación no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

La regulación sobre la medida permite de forma excepcional, en los casos de urgencia en que se aprecie un interés constitucional legítimo que la haga imprescindible, que la Policía Judicial examine directamente los datos contenidos en el dispositivo incautado, en ausencia de autorización judicial previa, pero con la obligación de comunicarlo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida (art. 588 sexies c 4º LECrim)⁴⁹.

Esta exigencia de motivación individualizada es analizada en la SAP de Madrid 382/2015 de 21 de mayo, donde la defensa instó la nulidad de la diligencia de volcado de datos almacenados en los dispositivos USB incautados al acusado, debido a la inexistencia de autorización judicial específica al respecto. En ese caso, la mayoría de los dispositivos fueron aprehendidos durante la diligencia de entrada y registro, sin embargo, uno de los USB fue incautado posteriormente, al momento de la detención del investigado. La Audiencia estableció que en cualquier caso es necesaria la autorización judicial habilitante para el registro de los dispositivos incautados, indicando con respecto de los hallados en el domicilio del investigado que existió tal habilitación, por lo que el volcado de la información contenida en los mismos se produjo bajo cobertura legal, habiéndose solicitado por la Policía una autorización para practicar dicha diligencia. Sin embargo, en relación al acceso de la información contenida en el USB incautado con motivo de la detención del investigado, la Audiencia entendió que dicho acceso no contaba con la necesaria cobertura judicial, ya que se realizó con posterioridad a la diligencia de entrada y registro y no se solicitó ampliación para el acceso del nuevo dispositivo

⁴⁹ GONZÁLEZ-CUELLAR SERRANO, N. y MARCHENA GÓMEZ, M., *op. cit.* Pág. 373.

incautado. En conclusión, la Audiencia indicó que, al tratarse de una medida restrictiva de derechos fundamentales, no puede entenderse la autorización judicial concedida tácitamente⁵⁰.

En esta línea, el TS reflexiona sobre la reforma de la LO 13/2015, en relación al art. 588 sexies a LECrim, entendiendo que *“se trata, por tanto, de una regulación rupturista, que pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia, incluso cuando desbordara el contenido material del derecho reconocido en el art. 18.2 de la CE. Lo que el legislador pretende, por tanto, es que el Juez de instrucción exteriorice de forma fiscalizable las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros”*⁵¹.

En contraposición, nada se regula sobre la conservación de la cadena de custodia de los dispositivos intervenidos, dejando así a la libre disposición del Juez y de la Policía Judicial el modo en que se llevará a cabo, a pesar de la relevancia que supone respecto a las garantías procesales del investigado⁵².

7.3. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.

La autorización judicial exigida por el art. 588 sexies a LECrim también será necesaria para aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes informarán al juez sobre la incautación de tales efectos y éste, si considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización (art. 588 sexies b LECrim).

⁵⁰ MARTÍN MARTÍN DE LA ESCALERA, A.M., *op. cit.* Pág. 7 y 8.

⁵¹ STS 864/2015, de 10 de diciembre, FJ 7.

⁵² RUBIO ALAMILLO, J. *op. cit.* Pág. 6.

7.4. Autorización judicial.

El art. 588 sexies c LECrim dispone que la resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos de almacenamiento masivo de información deberá fijar los siguientes aspectos:

- Los términos y el alcance del registro.
- Autorización, en su caso, para la realización de copias de los datos informáticos.
- Las condiciones necesarias para asegurar la integridad de los datos.
- Las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

Se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos. Se exceptúan los casos en que dichos soportes constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen.

El legislador ha previsto la posibilidad de que se amplíe el objeto del registro, mediante una nueva autorización judicial, salvo que la ampliación ya estuviera prevista en la autorización inicial. Este supuesto se produce cuando quienes llevan a cabo el registro o tienen acceso al sistema de información o a una parte del mismo, tienen razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él. En caso de urgencia, la Policía Judicial o el fiscal podrán llevar a cabo el registro (sin autorización judicial previa sobre la ampliación), informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

A continuación, en el apartado quinto del presente artículo, se vuelve a hacer referencia al deber de colaboración anteriormente mencionado, estableciendo que las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos

informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia. No obstante, esta obligación no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional.

8. RÉGIMEN JURÍDICO DE LOS REGISTROS REMOTOS SOBRE EQUIPOS INFORMÁTICOS.

Los registros remotos sobre equipos informáticos están regulados en el Capítulo IX del Título VIII del Libro II de la LECrim, introducido en el artículo único, apartado dieciocho, de la Ley Orgánica 13/2015.

Se trata una de las diligencias más novedosas y relevantes introducidas por la reforma, consistente en el acceso y registro, remota o telemáticamente, de equipos electrónicos o informáticos mediante la instalación previa en el mismo de un software que permite a la Policía Judicial acceder al contenido y transmitirlo a otro equipo informático, que suele ser el de la autoridad encargada de la investigación⁵³.

A diferencia de los registros convencionales sobre un dispositivo, por los que se obtiene la información contenida en éste en un momento determinado, los registros remotos permiten efectuar una intervención prolongada en el tiempo, siendo de mayor grado la injerencia en el derecho al secreto de las comunicaciones, a la intimidad, a la protección de datos y a la propia imagen del sujeto investigado. Es por ello que el legislador ha introducido una regulación estricta al respecto, reforzando las garantías procesales a fin de proteger los derechos fundamentales en juego.

8.1.Presupuestos.

El art. 588 septies a LECrim establece los presupuestos para la adopción de la medida de registro de equipos informáticos, separándose de la regla general aplicada en otras medidas como la intervención de las comunicaciones telefónicas, donde se tiene en consideración la gravedad del delito⁵⁴, atendiendo en este caso a alguno de los siguientes delitos:

- a) Delitos cometidos en el seno de organizaciones criminales.
- b) Delitos de terrorismo.

⁵³ ORTIZ PRADILLO, J.C., “Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica” en PÉREZ GIL, J., *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*. La Ley, Madrid, 2012, Pág.4.

⁵⁴ “Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión”.

- c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
- d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
- e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

En consecuencia, para que el juez competente autorice la medida, esto es, la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, la investigación deberá perseguir alguno de los delitos descritos anteriormente.

En cuanto a los requisitos que debe cumplir la resolución judicial que autorice el registro, ésta deberá especificar:

- a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.
- b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
- c) Los agentes autorizados para la ejecución de la medida.
- d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
- e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Al igual que ocurría en los registros de dispositivos de almacenamiento masivo de información, el Juez podrá acordar la ampliación de los términos de la medida, cuando los

agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo.

8.2. Deber de colaboración.

El art. 588 septies b LECrim vuelve a hacer referencia al deber de colaboración, de forma muy similar a lo fijado para los registros de dispositivos de almacenamiento masivo de información, estableciendo en este caso que los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización. Todos éstos sujetos requeridos para prestar colaboración tienen la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. Además, quedan sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e.

En relación a dicho deber, las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.

Todo lo expuesto anteriormente respecto al deber de colaboración no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

8.3. Duración de la medida.

El art. 588 septies c LECrim fija como duración máxima de la medida el plazo de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

Si comparamos la duración de esta medida con las estudiadas anteriormente, podemos observar que se establece un plazo máximo inferior al del resto, puesto a que la injerencia en los derechos fundamentales del sujeto investigado es de mayor intensidad.

8.4. Técnicas de obtención de información a través de registros remotos sobre dispositivos informáticos.

Existe una gran diferencia entre el acceso a las comunicaciones telefónicas o de mensajería a través de cable o de redes móviles, y el acceso a la información contenida en correos electrónicos, redes sociales como Facebook, y aplicaciones de mensajería instantánea como WhatsApp, donde la labor investigadora se complica.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGT), en su art. 39, impone el deber de garantizar el secreto de las comunicaciones a los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, conforme a los arts. 18.3 y 55.2 CE, debiendo adoptar las medidas necesarias a tal efecto. En las interceptaciones que se autoricen, los operadores deberán actuar según lo dispuesto en el art. 579 LECrim, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

Continúa el citado precepto que dicha intervención deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El problema surge respecto al modo en que la información obtenida mediante la intervención llega al agente facultado, la cual debe presentarse en un formato claro y susceptible de ser entendido. Pero cuando se trata de las señales que viajan por Internet, el acceso a la

información que contienen resulta muy dificultoso, ya que normalmente se encuentran encriptadas o cifradas. En consecuencia, en estos casos es fundamental el deber de colaboración establecido en el art. 588 ter e LECrim, que permite acudir a otros profesionales para que descrypten o descifren las señales interceptadas y obtener así la información de forma legible e interpretable. Estas técnicas se han convertido de vital importancia para que la medida de investigación llegue a un buen fin, como el nuevo sistema Evident X-Stream, una herramienta que funciona bajo vigilancia legalmente autorizada, recopilando, decodificando y analizando los datos obtenidos, previa autorización judicial y con sometimiento a las previsiones legales sobre la materia. Se basa en la colaboración de los colaboradores de Internet (IPSS) y las operadoras de telecomunicación (CSPs). Mediante autorización judicial, se establecen estructuras que recopilan los datos de los usuarios operados por compañías tales como Movistar, Orange o Vodafone a través del uso del sistema Evident X-Stream.

Otro tipo de herramientas utilizadas para acceder de modo remoto a la información contenida en dispositivos informáticos son los spyware o troyanos.

9. CONCLUSIONES.

Después del estudio de la LO 13/2015, de modificación de la LECrim (Ley 1/1882), en lo referente a las nuevas medidas de investigación tecnológica, la regulación dada en el texto procesal supone una normativa transgresora en España, que trata de dar respuesta a las controversias suscitadas en torno a la protección de los derechos fundamentales en los procedimientos de investigación penales a través de la interceptación de las comunicaciones y del espionaje informático. La necesidad de luchar contra los delitos informáticos, actualizar el proceso penal y cubrir ciertas lagunas legales con el objetivo de cumplir con los principios de seguridad jurídica y legalidad han dado como resultado la modificación de la LECrim.

El elenco de medidas es muy variado, desde la interceptación de las telecomunicaciones completa, hasta diligencias más arriesgadas como la instalación de virus espía o utilización de drones en lugares al aire libre. Todas estas novedades pretenden detener la comisión de hechos delictivos en la Red.

Nuestra valoración en torno a las nuevas medidas de investigación tecnológica introducidas por la LO 13/2015 es positiva, ya que finalmente se ha logrado dotar de cobertura legal a un conjunto de prácticas necesarias para la persecución de los ciberdelitos, que hasta entonces no contaban con una regulación expresa, lo que tenía como consecuencia que las diligencias practicadas fueran obtenidas con vulneración de los derechos fundamentales y no pudieran ser utilizadas como una prueba de cargo.

La nueva redacción de la LECrim presenta numerosas ventajas, entre las que destacan la introducción de nuevas figuras de investigación, como el uso de drones, el agente encubierto o software espía; así como el rango de protección otorgado a los derechos fundamentales de los sujetos investigados, regulándose la práctica de las diligencias de investigación tecnológica mediante Ley Orgánica. Además, ha sido acertada la adaptación del lenguaje utilizado para establecer la nueva estructura y catálogo de medidas, adaptado todo ello a los nuevos tiempos y a la rápida evolución tecnológica.

No obstante, algunas cuestiones continúan quedando indeterminadas, por lo que resulta preciso su desarrollo a través de la jurisprudencia. Uno de estos aspectos sería la prórroga de ciertas medidas como la interceptación de las comunicaciones. En casos como este, generaría mayor seguridad a la sociedad si se estableciera un límite máximo para la práctica de ciertas

diligencias, de modo que los ciudadanos no sintieran gravemente vulnerado su derecho a la intimidad y al secreto de las comunicaciones. Asimismo, cada caso debería ser valorado individualmente por el Juez a la hora de alargar temporalmente la utilización de una medida, con el fin de dar la máxima protección a los derechos de los sujetos investigados.

De otro lado, nos ha llamado la atención la ausencia de una regulación general para todas las medidas sobre el acceso de las partes, así como de los terceros afectados, a las grabaciones una vez finalizada la práctica de la misma. La norma sí prevé esta opción en el caso de las intervenciones telefónicas, estableciendo en el art. 588 ter i LECrim que, una vez alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso. Por consiguiente, en cuanto la actual regulación no prevé el citado acceso a las grabaciones para el resto de las figuras de intervención tecnológicas, resulta preciso dar conocimiento al investigado sobre las diligencias practicadas y la información obtenida, ya que se trata de prácticas que interfieren en sus derechos fundamentales y que el sujeto desconoce hasta que las mismas han finalizado, lo que podría influir negativamente en su derecho de defensa.

En el nuevo texto también se utilizan términos indeterminados como que “cualquier persona” puede dar apoyo en la práctica de las diligencias para que lleguen a buen fin. Con ello, parece dar la sensación de que la consecución del fin de la medida se encuentra muy por encima de cualquier tipo de garantía y precaución debida en su práctica; pero no debemos olvidar que el ámbito de las mismas interfiere en los derechos fundamentales del investigado, por lo que no todo sería válido con tal de poder realizar este tipo de diligencias. Estamos de acuerdo en que la Justicia debe modernizarse y adaptarse a las novedades del presente, pero no de cualquier forma ni a cualquier precio, ya que se pone en riesgo el reducto más íntimo del investigado.

Por otro lado, desde nuestro punto de vista, la figura del agente encubierto continúa siendo confusa e insuficiente, y consideramos que debería regularse más exhaustiva y coherentemente con la naturaleza de la medida, eliminando cualquier tipo de laguna legal y evitando así generar inseguridad jurídica con la utilización de esta herramienta.

Con todo lo anterior, y para concluir nuestra reflexión, queremos destacar nuestra satisfacción con la adaptación de nuestro texto procesal a la realidad actual, se trata de una legislación pionera en España, la cual venía siendo necesaria desde hace ya varios años y que finalmente ha logrado cubrir los vacíos legales que suscitaban tantas controversias a la hora de practicar ciertas diligencias de investigación. A pesar de la ausencia de regulación expresa sobre la materia, este tipo de actuaciones se practicaban, lo cual inducía a una vulneración de los derechos fundamentales y a que fueran los tribunales quienes tuvieran que decidir sobre la precedencia de la medida. Aplaudimos por ello que por fin el legislador haya introducido toda una serie de novedades que permitan la práctica de las diligencias expuestas a lo largo de nuestro estudio bajo el principio de legalidad. No obstante, en un mundo globalizado donde no existen fronteras cibernéticas, debería darse un paso más y crear una regulación, al menos, a nivel de la Unión Europea, para facilitar de ese modo la actuación de los agentes de la autoridad y que la persecución de los delitos informáticos sea más eficaz.

BIBLIOGRAFÍA

Doctrina:

- ❖ CASANOVA MARTÍ, R. “La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos”, en *Diario La Ley*, núm. 8674, 2016.
- ❖ CORTÉS LÓPEZ, M.J., “Grabación de Conversaciones y Secreto de las Comunicaciones: Estudio de la sentencia del Tribunal Constitucional de fecha 22 de Septiembre de 2014”, en *Revista de Derecho vLex*. Núm. 132. Mayo 2015.
- ❖ DELGADO MARTÍN, J., “Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015”, en *Diario La Ley*, núm. 8693, 2016.
- ❖ FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.A., *Cuestiones actuales del Derecho Procesal*. Dykinson, Barcelona, 2015.
- ❖ GONZÁLEZ-CUELLAR SERRANO, N. y MARCHENA GÓMEZ, M., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Castillo de Luna, 2015.
- ❖ JAÉN VALLEJO, M. y PERRINO PÉREZ, A.L., “Medidas de investigación tecnológica”, en *La Reforma Procesal Penal de 2015*. Dykinson Madrid, 2015.
- ❖ JIMENEZ SEGADO, C. y PUCHOL AIGUABELLA, M. “Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección de datos”, en *Diario La Ley*, núm. 8676, 2016.
- ❖ MARTÍN MARTÍN DE LA ESCALERA, A.M., *El registro de dispositivos de almacenamiento masivo de la información*.
- ❖ ORTIZ PRADILLO, J.C., “Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica”, en PÉREZ GIL, J., *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*. La Ley, Madrid, 2012.

- ❖ RODRIGUEZ LAINZ, J.L. “La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014”, en *Diario La Ley*, núm. 8465, 2015.
- ❖ RUBIO ALAMILLO, J. “La informática en la reforma de la Ley de Enjuiciamiento Criminal”, en *Diario La Ley*, núm. 8662, 2015.

Recursos web:

- ❖ *Dispositivos de almacenamiento masivo* (en línea)
http://www.informaticamoderna.com/Disp_almacen.htm (consulta 10 de abril de 2018).

Legislación:

- ❖ Constitución Española.
- ❖ Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- ❖ Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Jurisprudencia:

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- ❖ STEDH, de 18 de febrero de 2003, asunto Prado Bugallo contra España.
- ❖ STEDH, de 16 de febrero de 2000, asunto Amann contra Suiza.

TRIBUNAL CONSTITUCIONAL

- ❖ STC 39/1999, de 22 de marzo.
- ❖ STC 49/1999, de 5 de abril.
- ❖ STC 14/2001, de 29 de enero.
- ❖ STC 299/2001, de 11 de diciembre.

- ❖ STC 82/2002, de 22 de abril.
- ❖ STC 120/2002, de 20 de mayo.
- ❖ STC 184/2003, de 23 de octubre.
- ❖ STC 26/2006, de 30 de enero.
- ❖ STC 197/2009, de 28 de septiembre.
- ❖ STC 26/2010, de 27 de abril.
- ❖ STC 145/2014, de 22 de septiembre.

TRIBUNAL SUPREMO

- ❖ STS 1769/2003, de 29 de diciembre (ROJ 8508/2003).
- ❖ STS 55/2007, de 23 de enero (ROJ 605/2007).
- ❖ STS 130/2007, de 19 de febrero (ROJ 1962/2007).
- ❖ STS 209/2007, de 9 de marzo (ROJ 2253/2007).
- ❖ STS 739/2008, de 12 de noviembre de 2008 (ROJ 6677/2008).
- ❖ STS 688/2008, de 30 de octubre (ROJ 5779/2008).
- ❖ STS 239/2010, de 24 de marzo (ROJ 1738/2010).
- ❖ STS 680/2010, de 14 de julio (ROJ 3944/2010).
- ❖ STS 663/2011, de 7 de julio (ROJ 5170/2011).
- ❖ STS 343/2012, de 30 de abril (ROJ 5706/2012).
- ❖ STS 712/2012, de 26 de septiembre (ROJ 6245/2012).
- ❖ STS 298/2013, de 13 de marzo (ROJ 1885/2013).
- ❖ STS 503/2013, de 19 de junio (ROJ 3275/2013).
- ❖ STS 686/2013, de 29 de julio (ROJ 4152/2013).
- ❖ STS 695/2013, de 22 de julio (ROJ 4490/2013).

- ❖ STS 793/2013, de 28 de octubre (ROJ 5249/2013)
- ❖ STS 938/2013, de 10 de diciembre (ROJ 6208/2013).
- ❖ STS 1029/2013, de 18 de diciembre (ROJ 6563/2013)
- ❖ STS 250/2014, de 14 de marzo (ROJ 1287/2014).
- ❖ STS 145/2014, de 22 de septiembre (ROJ 835/2014).
- ❖ STS 413/2015, de 30 de junio (ROJ 3177/2015).
- ❖ STS 128/2015, de 5 de febrero (ROJ 1098/2015).
- ❖ STS 864/2015, de 10 de diciembre (ROJ 5809/2015).
- ❖ STS 204/2016, de 10 de marzo (ROJ 1218/2016).
- ❖ STS 395/2016, de 10 de mayo (ROJ 2131/2016).
- ❖ STS 404/2016, de 1 de mayo (ROJ 2146/2016).
- ❖ STS 107/2017, de 21 de enero (ROJ 687/2017).
- ❖ STS 297/2017, de 26 de abril (ROJ 1643/2017).
- ❖ STS 747/2017, de 21 de noviembre (ROJ 24210/2017).

AUDIENCIA PROVINCIAL

- ❖ SAP de Madrid 382/2015 de 21 de mayo.